(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－261748
（P2002－261748A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｈ０４Ｌ　9/00	６０１Ｃ	５Ｊ１０４
Ｈ０４Ｌ　9/32			６７１	

審査請求　未請求　請求項の数22　ＯＬ　（全 18 頁）

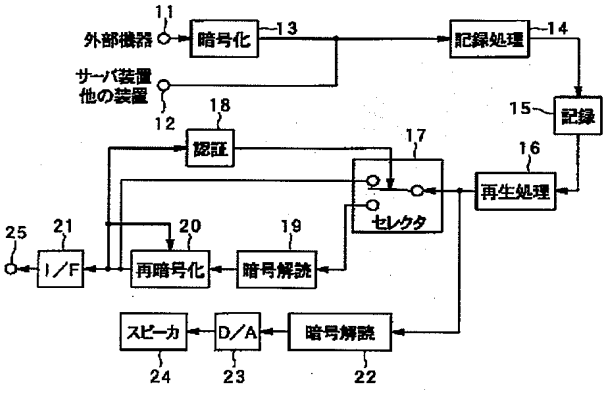
(21)出願番号　特願2001－163126(P2001－163126)
(22)出願日　平成13年５月30日(2001.5.30)
(31)優先権主張番号　特願2000－403467(P2000－403467)
(32)優先日　平成12年12月28日(2000.12.28)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　猪口　達也
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100067736
弁理士　小池　晃　（外２名）

最終頁に続く

(54)【発明の名称】　データ送信装置及び方法並びにデータ記録装置及び方法

(57)【要約】
【課題】　ネットワーク内のサーバ装置を介在させてディジタルコンテンツのやり取りを行う際にもデータの無断複写を防止することができる。
【解決手段】　データの送信先の装置の認証を取る認証回路１８と、暗号化されたデータを解読する暗号解読回路１９と、暗号解読回路１９で解読されたデータを再暗号化する再暗号化回路２０とを備える。記録再生装置２は、認証回路１８によりデータの送信先の装置の認証が取れたとき、記録媒体から読み出した暗号化されたデータを暗号解読回路１９で解読すると共に送信先の装置の固有鍵データを取得し、この取得した固有鍵データを用いて再暗号化回路２０でデータを再暗号化して通信Ｉ／Ｆ２１から送信する。したがって、サーバ装置に一時的にデータが記録され、このデータが権限無き第三者の端末装置にダウンロードされても、再生されることを防止できる。



【特許請求の範囲】

【請求項１】　記録媒体に記録された暗号化されたデータを読み出し再生処理を施す再生処理手段と、
上記データの送信先の装置の認証を取る認証手段と、
上記再生処理手段で再生処理が施された暗号化されたデータを解読する暗号解読手段と、
上記暗号解読手段で解読されたデータを再暗号化する再暗号化手段と、
上記再暗号化手段により暗号化されたデータを出力する出力手段とを備え、
上記認証手段により上記データの送信先の装置の認証が取れたとき、上記記録媒体から読み出し再生処理が施された暗号化されたデータを上記暗号解読手段で解読すると共に上記送信先の装置の固有鍵データを取得し、この取得した固有鍵データを用いて上記再暗号化手段で上記データを再暗号化して上記出力手段から送信するデータ送信装置。

【請求項２】　上記暗号解読手段の前段には、上記暗号化手段により暗号化されたデータをそのまま上記出力手段より出力できるようにする切換手段が設けられ、
上記データの送信先の装置の認証を取らないとき又は認証が取れなかったとき、上記切換手段は、上記記録媒体から読み出し再生処理が施された暗号化されたデータをそのまま上記出力手段より出力できるようにする請求項１記載のデータ送信装置。

【請求項３】　上記暗号化されたデータの一部は、暗号化処理が施されていない請求項１記載のデータ送信装置。

【請求項４】　記録媒体に記録された暗号化されたデータを読み出し再生処理を施すステップと、
上記記録媒体に記録された暗号化されたデータを送信するとき、送信先の装置の認証を取るステップと、
上記データの送信先の装置の認証が取れたとき、上記送信先の装置より、この送信先の装置の固有鍵データを取得するステップと、
上記データの送信先の装置の認証が取れたとき、上記再生処理が施された暗号化されたデータを解読するステップと、
上記解読されたデータを上記送信先の固有鍵データを用いて再暗号化するステップと、
上記再暗号化されたデータを出力するステップとを有するデータ送受信方法。

【請求項５】　上記データの送信先の装置の認証を取らないとき又は認証が取れなかったとき、上記記録媒体から読み出し再生処理が施された暗号化されたデータをそのまま出力する請求項４記載のデータ送信方法。

【請求項６】　上記暗号化されたデータの一部は、暗号化処理が施されていない請求項４記載のデータ送信方法。

【請求項７】　記録媒体に記録された暗号化されたデータを読み出し再生処理を施す再生処理手段と、
上記データの送信先の装置の認証を取る認証手段と、
上記データを出力する出力手段とを備え、
上記認証手段により上記データの送信先の装置の認証が取れたとき、上記暗号化されたデータを上記出力手段よりそのまま出力するデータ送信装置。

【請求項８】　上記データの送信先の装置の認証を取らないとき又は認証が取れなかったとき、上記出力手段からのデータの出力を禁止する請求項７記載のデータ送信装置。

【請求項９】　更に、上記データの送信先となる他の装置の認証を取る更なる認証手段と、
上記再生処理手段で再生処理された暗号化されたデータを解読する暗号解読手段と、
上記暗号解読手段で解読されたデータを再暗号化する再暗号化手段とを備え、
上記認証手段が上記データの送信先の装置の認証を取らないとき又は認証が取れなかったときで、上記更なる認証手段により送信先の装置の認証が取れたとき、上記記録媒体から読み出し再生処理が施された暗号化されたデータを上記暗号解読手段で解読し、上記送信先の装置の固有鍵データを取得し、この取得した固有鍵データを用いて上記再暗号化手段で上記データを再暗号化して上記出力手段から出力する請求項７記載のデータ送信装置。

【請求項１０】　記録媒体に記録された暗号化されたデータを読み出し再生処理を施すステップと、
上記記録媒体に記録された暗号化されたデータを送信するとき、送信先の装置の認証を取るステップと、
上記データの送信先の装置の認証が認証手段で取れたとき、上記暗号化されたデータをそのまま出力するステップとを有するデータ送信方法。

【請求項１１】　上記データの送信先の装置の認証を取らないとき又は認証が取れなかったとき、上記データの出力を禁止する請求項１０記載のデータ送信方法。

【請求項１２】　上記データの送信先の装置の認証を取らないとき又は認証が取れなかったときで、更なる認証手段により送信先の装置の認証が取れたとき、上記記録媒体から読み出し再生処理が施された暗号化されたデータを暗号解読し、上記送信先の装置の固有鍵データを取得し、この取得した固有鍵データを用いて上記データを再暗号化して出力する請求項１０記載のデータ送信方法。

【請求項１３】　記録媒体に記録された暗号化されたデータを読み出し再生処理を施す再生処理手段と、
上記データの送信先の認証を取る認証手段と、
上記認証手段で認証した上記送信先の装置の種類を判別する判別手段と、
上記再生処理手段で再生処理された暗号化されたデータを解読する暗号解読手段と、
上記暗号解読手段で解読されたデータを認証の取れた送

信先の装置より取得した装置の固有鍵データで再暗号化する再暗号化手段と、
上記再生処理手段で再生処理された暗号化されたデータをそのまま出力する第１の出力手段と、
上記再暗号化手段で再暗号化されたデータを出力する第２の出力手段とを備え、
上記判別手段は、送信先の装置が第１の装置であると判断したとき、上記第１の出力手段より上記再生処理手段で再生処理された暗号化されたデータをそのまま上記第１の装置に出力するようにし、
送信先の装置が第２の装置であると判断したとき、上記再生処理手段で再生処理された暗号化されたデータを上記暗号解読手段で解読し、上記第２の装置より取得した固有鍵データを用いて上記再暗号化手段で再暗号化して上記第２の出力手段より上記第２の装置に出力するデータ送信装置。

【請求項１４】　上記第１の装置は、専用機器であり、上記第２の装置は、汎用機器である請求項１３記載のデータ送信装置。

【請求項１５】　上記第１の装置は、少なくとも暗号解読手段がハードウェアで構成されており、上記第２の装置は、少なくとも暗号解読手段がソフトウェアにより構成されている請求項１３記載のデータ送信装置。

【請求項１６】　記録媒体に記録された暗号化されたデータを読み出し再生処理を施すステップと、
上記データの送信先の装置の認証を取るステップと、
認証した上記送信先の装置の種類を判別するステップと、
判別結果が第１の装置であるとき、再生処理された暗号化されたデータをそのまま第１の装置に出力するステップと、
判別結果が第２の装置であるとき、再生処理された暗号化されたデータを暗号解読し、上記第２の装置の固有鍵データで再暗号化して上記第２の装置に出力するステップとを有するデータ送信方法。

【請求項１７】　上記第１の装置は、専用機器であり、上記第２の装置は、汎用機器である請求項１６記載のデータ送信方法。

【請求項１８】　上記第１の装置は、少なくとも暗号解読手段がハードウェアで構成されており、上記第２の装置は、少なくとも暗号解読手段がソフトウェアにより構成されている請求項１６記載のデータ送信方法。

【請求項１９】　入力されたデータより無断複製防止情報を抽出し更新する抽出更新手段と、
上記抽出更新手段で上記無断複製防止情報が更新されたデータに記録処理を施し、記録媒体に記録する記録処理手段とを備え、
入力された上記データを再生処理可能なとき、上記抽出更新手段は、上記無断複写防止情報を更新すると共に、上記無断複写防止情報に基づいて上記記録処理手段を制御するデータ記録装置。

【請求項２０】　上記無断複写防止情報は、ＳＣＭＳ（Serial Copy Management System）情報であり、
上記抽出更新手段は、上記ＳＣＭＳ情報が複写自由であるとき、上記入力されたデータをそのまま上記記録媒体に記録するように上記記録処理手段を制御し、上記ＳＣＭＳ情報が１世代複写可能情報であるとき、該ＳＣＭＳ情報を複写禁止に書き換えると共に上記入力されたデータに所定の記録処理を施して上記記録媒体に記録するように上記記録処理手段を制御し、上記ＳＣＭＳ情報が複写禁止情報であるとき、上記記録処理手段の上記記録媒体への記録を禁止する請求項１９記載のデータ記録装置。

【請求項２１】　入力されたデータより無断複製防止情報を抽出し更新するステップと、
無断複製防止情報が更新されたデータに記録処理を施し、記録媒体に記録するステップと、
上記入力されたデータの再生処理が可能なとき、上記無断複写防止情報に基づいて記録処理を行うステップとを有するデータ記録方法。

【請求項２２】　上記無断複写防止情報は、ＳＣＭＳ（Serial Copy Management System）情報であり、
上記ＳＣＭＳ情報が複写自由であるとき、上記入力されたデータをそのまま上記記録媒体に記録し、上記ＳＣＭＳ情報が１世代複写可能情報であるとき、該ＳＣＭＳ情報を複写禁止に書き換えると共に上記入力されたデータに所定の記録処理を施して上記記録媒体に記録し、上記ＳＣＭＳ情報が複写禁止情報であるとき上記記録媒体への記録を禁止する請求項２１記載のデータ記録方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタルコンテンツ等のデータの無断複写を防止するデータ送信装置及び方法並びにデータ記録装置及び方法に関する。

【０００２】

【従来の技術】従来、再生専用の光ディスクからオーディオデータ等のディジタルコンテンツをディジタル信号のまま記録可能な光磁気ディスクに複写することが行われている。光磁気ディスクの記録再生装置は、光ディスクの再生装置に専用ケーブルで接続しディジタルコンテンツを複写する際に、このディジタルコンテンツに一回のみ複写を可能となす無断複写防止情報を記録禁止に更新し、著作権管理を行うようにしている。したがって、光磁気ディスクに記録されている光ディスクから複写したディジタルコンテンツは、更に光磁気ディスクに複写することができないようになっている。

【０００３】また、インターネット、ＬＡＮ(local area network)等のネットワークを介してパーソナルコンピュータ等の端末装置間でディジタルコンテンツのやり取りが行われている。この場合、送信側の端末装置は、受

信側の端末装置のアドレスと共にサーバ装置にディジタルコンテンツをアップロードし、受信側の端末装置は、サーバ装置に記憶されている自分宛のディジタルコンテンツをダウンロードする。このようなネットワークを介在させたディジタルコンテンツのやり取りでは、ディジタルコンテンツの複写回数は全く管理されていないことが多い。

【０００４】

【発明が解決しようとする課題】上述したネットワークを介在させてディジタルコンテンツをやり取りするシステムは、再生専用の光ディスクから記録可能な光磁気ディスクにディジタルコンテンツを複写するシステムのように専用の光磁気ディスクの記録再生装置を用いるものではなく、汎用コンピュータを用いるものであるから、複写するディジタルコンテンツに無断複写防止情報を付加し、複写した際に無断複写防止情報の更新を行うようにし、著作権管理を行うことは困難である。

【０００５】本発明の目的は、有形な記録媒体を用いること無く、ネットワーク内のサーバ装置を介在させて間接的に又は装置間で有線若しくは無線で直接的にディジタルコンテンツのやり取りを行う際にもデータの無断複写を防止する等の著作権管理を行うことができるデータ送信装置及び方法並びにデータ記録装置及び方法を提供することにある。

【０００６】

【課題を解決するための手段】本発明に係るデータ送信装置は、上述した課題を解決すべく、記録媒体に記録された暗号化されたデータを読み出し再生処理を施す再生処理手段と、データの送信先の装置の認証を取る認証手段と、再生処理手段で再生処理が施された暗号化されたデータを解読する暗号解読手段と、暗号解読手段で解読されたデータを再暗号化する再暗号化手段と、再暗号化手段により暗号化されたデータを出力する出力手段とを備える。そして、認証手段によりデータの送信先の装置の認証が取れたとき、記録媒体から読み出し再生処理が施された暗号化されたデータを暗号解読手段で解読すると共に送信先の装置の固有鍵データを取得し、この取得した固有鍵データを用いて再暗号化手段でデータを再暗号化して出力手段から送信する。

【０００７】また、本発明に係るデータの送信方法は、上述した課題を解決すべく、記録媒体に記録された暗号化されたデータを読み出し再生処理を施すステップと、記録媒体に記録された暗号化されたデータを送信するとき、送信先の装置の認証を取るステップと、データの送信先の装置の認証が取れたとき、送信先の装置より、この送信先の装置の固有鍵データを取得するステップと、データの送信先の装置の認証が取れたとき、再生処理が施された暗号化されたデータを解読するステップと、解読されたデータを送信先の固有鍵データを用いて再暗号化するステップと、再暗号化されたデータを出力するステップとを有する。

【０００８】更に、本発明に係るデータ送信装置は、上述した課題を解決すべく、記録媒体に記録された暗号化されたデータを読み出し再生処理を施す再生処理手段と、データの送信先の装置の認証を取る認証手段と、データを出力する出力手段とを備える。そして、認証手段によりデータの送信先の装置の認証が取れたとき、暗号化されたデータを出力手段よりそのまま出力する。

【０００９】更にまた、本発明に係るデータの送信方法は、上述した課題を解決すべく、記録媒体に記録された暗号化されたデータを読み出し再生処理を施すステップと、記録媒体に記録された暗号化されたデータを送信するとき、送信先の装置の認証を取るステップと、データの送信先の装置の認証が認証手段で取れたとき、暗号化されたデータをそのまま出力するステップとを有する。

【００１０】更にまた、本発明に係るデータ送信装置は、上述した課題を解決すべく、記録媒体に記録された暗号化されたデータを読み出し再生処理を施す再生処理手段と、データの送信先の認証を取る認証手段と、認証手段で認証した送信先の装置の種類を判別する判別手段と、再生処理手段で再生処理された暗号化されたデータを解読する暗号解読手段と、暗号解読手段で解読されたデータを認証の取れた送信先の装置より取得した装置の固有鍵データで再暗号化する再暗号化手段と、再生処理手段で再生処理された暗号化されたデータをそのまま出力する第１の出力手段と、再暗号化手段で再暗号化されたデータを出力する第２の出力手段とを備える。そして、判別手段は、送信先の装置が第１の装置であると判断したとき、第１の出力手段より再生処理手段で再生処理された暗号化されたデータをそのまま第１の装置に出力するようにし、送信先の装置が第２の装置であると判断したとき、再生処理手段で再生処理された暗号化されたデータを暗号解読手段で解読し、第２の装置より取得した固有鍵データを用いて再暗号化手段で再暗号化して第２の出力手段より第２の装置に出力する。

【００１１】更にまた、本発明に係るデータの送信方法は、上述した課題を解決すべく、記録媒体に記録された暗号化されたデータを読み出し再生処理を施すステップと、データの送信先の装置の認証を取るステップと、認証した送信先の装置の種類を判別するステップと、判別結果が第１の装置であるとき、再生処理された暗号化されたデータをそのまま第１の装置に出力するステップと、判別結果が第２の装置であるとき、再生処理された暗号化されたデータを暗号解読し、第２の装置の固有鍵データで再暗号化して第２の装置に出力するステップとを有する。

【００１２】更に、本発明に係るデータ記録装置は、上述した課題を解決すべく、入力されたデータより無断複製防止情報を抽出し更新する抽出更新手段と、抽出更新手段で無断複製防止情報が更新されたデータに記録処理

を施し、記録媒体に記録する記録処理手段とを備える。そして、入力されたデータを再生処理可能なとき、抽出更新手段は、無断複写防止情報を更新すると共に、無断複写防止情報に基づいて記録処理手段を制御する。

【００１３】更にまた、本発明に係るデータ記録方法は、上述した課題を解決すべく、入力されたデータより無断複製防止情報を抽出し更新するステップと、無断複製防止情報が更新されたデータに記録処理を施し、記録媒体に記録するステップと、入力されたデータの再生処理が可能なとき、無断複写防止情報に基づいて記録処理を行うステップとを有する。

【００１４】

【発明の実施の形態】以下、本発明が適用されたデータ送受信システムについて、図面を参照して説明する。

【００１５】図１に示すように、このデータ送受信システム１は、オーディオデータ等のディジタルデータの記録再生を行うことができる記録再生装置２ａ，２ｂと、記録再生装置２ａ，２ｂが電気通信回線を介して接続されるネットワーク５内のサーバ装置３とを備える。

【００１６】サーバ装置３は、例えば一方の記録再生装置２ａからアップロードされたオーディオデータ等のディジタルデータをハードディスク等の記憶部に一時的に記憶し、他方の記録再生装置２ｂからのダウンロード要求を受信したとき、記憶部に記憶しているオーディオデータを記録再生装置２ｂに送信する。

【００１７】また、記録再生装置２ａと記録再生装置２ｂとは、ＩＥＥＥ(The Institute of Electronics Engineer,Inc.)１３９４規格等に準拠したインターフェースを用いて装置間に専用ケーブルを接続することで、サーバ装置３を介すること無く直接的にデータの送受信を行うことができる。

【００１８】ここで、記録再生装置２ａ，２ｂについて、図２を参照して説明する。なお、記録再生装置２ａと記録再生装置２ｂは、同じ構成を有するため、以下単に記録再生装置２ともいう。

【００１９】この記録再生装置２は、外部機器から出力されたオーディオデータ等のディジタルデータが入力される入力端子１１と、サーバ装置３からネットワーク５を介して又は他の記録再生装置２から暗号化されたディジタルデータが入力される入力端子１２とを有する。また、記録再生装置２は、入力端子１１から入力されたディジタルデータを暗号化する暗号化回路１３と、暗号化されたディジタルデータの記録処理を行う記録処理回路１４と、暗号化されたディジタルデータが記録されるハードディスク、記録可能な光ディスク、光磁気ディスク、半導体メモリ、ＩＣカード等からなる記憶部１５と、磁気ヘッド、光ピックアップ等の再生手段から読み出されたディジタルデータの再生処理を行う再生処理回路１６とを有する。

【００２０】また、この記録再生装置２は、サーバ装置３や他の記録再生装置２にディジタルデータを送信するための送信系として、暗号化されたディジタルデータをそのまま出力する経路と暗号化されたディジタルデータを再暗号化して出力する経路とを切り換えるセレクタ１７と、ディジタルデータの送信先の認証を取り認証結果に基づいてセレクタ１７を制御する認証回路１８と、暗号化されたディジタルデータを解読する暗号解読回路１９と、暗号解読回路１９で暗号解読されたディジタルデータを再暗号化する再暗号化回路２０と、サーバ装置３や他の記録再生装置２とデータ通信を行うための通信インターフェース（以下、単に通信Ｉ／Ｆともいう。）２１とを備える。

【００２１】更に、記録再生装置２は、記憶部１５に記録されたディジタルデータの再生系として、再生処理回路１６からの出力が入力される暗号解読回路２２と、暗号解読されたディジタルデータをディジタル信号からアナログ信号に変換するＤ／Ａコンバータ２３と、アナログ信号に変換されたデータを電気音響変換し出力するスピーカ２４とを備える。

【００２２】暗号化回路１３は、メモリに記憶されている装置個別鍵を用いて入力端子１１から入力されたディジタルデータを暗号化する。具体的に、この暗号化回路１３は、図３に示すように、乱数を発生する乱数発生回路３１と、乱数に基づいた関数を発生する関数回路３２と、コンテンツを暗号化するコンテンツ鍵を記憶するコンテンツ鍵用メモリ３３と、コンテンツ鍵を暗号化するために用いる共通鍵を記憶する共通鍵用メモリ３４と、記録再生装置２の固有の装置個別鍵を記録する装置個別鍵用メモリ３５と、共通鍵と装置個別鍵とで全ての記録再生装置２に共通する装置共通鍵を生成する装置共通鍵生成回路３６と、コンテンツ鍵でコンテンツを暗号化するコンテンツ暗号化回路３７と、装置共通鍵と乱数が与えられた関数とでコンテンツ鍵を暗号化するコンテンツ鍵暗号化回路３８とを備える。

【００２３】ディジタルデータが暗号化回路１３に入力されると、コンテンツ暗号化回路３７は、コンテンツ鍵用メモリ３３より所定のコンテンツ鍵を読み出し、このコンテンツ鍵を用いてタイトル等のヘッダを除き暗号化し、暗号化コンテンツを出力する。これと共に、乱数発生回路３１は、乱数を発生し、この乱数を関数回路３２に出力し、関数回路３２は、乱数に基づいて関数を発生する。また、装置共通鍵生成回路３６は、共通鍵用メモリ３４から共通鍵を読み出し、装置固有鍵用メモリ３５から装置固有鍵を読み出し、共通鍵と装置固有鍵とに基づいて装置共通鍵を生成する。コンテンツを暗号化するのに用いるコンテンツ鍵は、コンテンツ鍵暗号化回路３８よりコンテンツ鍵暗号化回路３８にも出力され、このコンテンツ鍵暗号化回路３８は、乱数が与えられて関数回路３２で発生された関数と装置共通鍵生成回路３６で生成された装置共通鍵とで、暗号化鍵を生成する。

【００２４】そして、暗号化回路１３は、次のようなパケットを生成する。すなわち、この暗号化回路１３により生成されるパケットは、暗号化されていないコンテンツのタイトル等からなるヘッダと、乱数発生回路３１で発生された乱数と、共通鍵用メモリ３４から出力された共通鍵と、コンテンツ鍵暗号化回路３８から出力された暗号化鍵と、コンテンツ暗号化回路３７から出力された暗号化コンテンツとから構成される。

【００２５】そして、以上のようなパケットを生成した暗号化回路１３は、記憶部１５に記録するための処理を施すためパケット単位で記録処理回路１４に出力する。記録処理回路１４には、暗号化回路１３で暗号化されたディジタルデータと、入力端子１２から入力されたサーバ装置３や他の記録再生装置２からの暗号化されたディジタルデータが入力される。この記録処理回路１４は、例えばこれら入力されたデータにエラー訂正符号化処理や変調処理を施し２値化する。そして、記録処理が施されたデータは、磁気ヘッドや光ピックアップ等の記録手段によって記憶部１５を構成する記録媒体に記録される。なお、記憶部１５は、装置本体に内蔵されたものであってもよく、装置本体に対して着脱可能であってもよい。

【００２６】また、記憶部１５に記憶されているデータも、磁気ヘッドや光ピックアップ等の再生手段によって記録媒体から読み出される。そして、読み出されたデータは、再生処理回路１６に出力される。再生処理回路１６は、再生手段から出力を２値化し、復調処理やエラー訂正処理を施して送信系の通信Ｉ／Ｆ２１又は再生系の暗号解読回路２２に出力する。

【００２７】認証回路１８は、送信先の記録再生装置２の認証を取り、その認証結果に基づいてセレクタ１７を切換制御する。また、認証回路１８は、送信先の記録再生装置２の認証が取れたときであっても、ディジタルデータをサーバ装置３を介して他の記録再生装置２に送信するか専用ケーブルで直接的に記録再生装置２に送信するかでセレクタ１７の切換制御を行う。セレクタ１７は、認証回路１８で認証が取れなかったときと、認証が取れ他の記録再生装置２に直接的にディジタルデータを出力するとき、ディジタルデータを暗号化されたまま出力できるように切り換え、認証が取れサーバ装置３を介して他の記録再生装置２に出力するとき、再暗号化をすることができるように切り換える。

【００２８】送信系を構成する暗号解読回路１９は、ディジタルデータを送信する際、送信先より取得した送信先の記録再生装置２の装置個別鍵で再暗号化するため上述した暗号化回路１３で暗号化されたディジタルデータを解読し、再暗号化回路２０に出力する。具体的に、この暗号解読回路２９は、図４に示すように、パケット中の乱数に基づいて関数を発生する関数回路４１と、上記暗号化回路１３の装置個別鍵用メモリ３５と同じ鍵が記憶されている装置個別鍵用メモリ４２と、パケット中の共通鍵と装置個別鍵用メモリ４２から読み出された装置個別鍵とにより装置共通鍵を生成する装置共通鍵生成回路４３と、関数回路４１で発生された関数と装置共通鍵生成回路４３で生成された装置共通鍵とでパケット中の暗号化鍵を解読する暗号化鍵解読回路４４と、暗号化鍵解読回路４４で解読されたコンテンツ鍵に基づいてパケット中の暗号化コンテンツを解読するコンテンツ解読回路４５とを備える。

【００２９】暗号解読回路１９に暗号化されたディジタルデータが入力されると、関数回路４１は、パケット中の乱数に基づいて関数を発生し、装置共通鍵生成回路４３は、パケット中の共通鍵と装置個別鍵用メモリ４２より装置個別鍵とを読み出し、装置共通鍵を生成し、暗号化鍵解読回路４４に出力する。暗号化鍵解読回路４４は、関数回路４１で発生された関数と装置共通鍵とによりパケット中より読み出した暗号化鍵を解読し、コンテンツ鍵を生成し、コンテンツ解読回路４５に出力する。コンテンツ解読回路４５は、パケット中より暗号化コンテンツを読み出し、これをコンテンツ鍵を用いて解読する。なお、パケット中のヘッダは、暗号化されていないので暗号解読回路１９は、そのままパケット中より読み出す。そして、暗号解読回路１９は、暗号解読後のディジタルデータを再暗号化回路２０に出力する。

【００３０】再暗号化回路２０は、認証が取れサーバ装置３を介して他の記録再生装置２に出力するとき、送信先の記録再生装置２から装置個別鍵を取得し、この装置個別鍵を用いて出力するディジタルデータを再暗号化する。この再暗号化回路２０は、上記図３に示す暗号化回路１３とほぼ同じ構成を有するため、詳細は省略するが装置共通鍵生成回路３６には、装置個別鍵用メモリ３５からではなく、ディジタルデータの送信先の他の記録再生装置２の装置個別鍵用メモリ３５から読み出された送信先の装置個別鍵が入力される。そして、再暗号化回路２０は、上述したように、暗号化されていないヘッダと、乱数発生回路３１で発生された乱数と、共通鍵用メモリ３４から出力された共通鍵と、コンテンツ鍵暗号化回路３８から出力された暗号化鍵と、コンテンツ暗号化回路３７から出力された暗号化コンテンツとからなるパケットを生成し、通信Ｉ／Ｆ２１に出力する。

【００３１】通信Ｉ／Ｆ２１は、例えばサーバ装置３に送信するとき、ＴＣＰ／ＩＰ（transmission control protocol/internet protocol）等の伝送プロトコルを実行し、サーバ装置３に再暗号化されたディジタルデータを出力端子２５を介して送信し、また、専用ケーブルで直接的に他の記録再生装置２に送信するとき、ＩＥＥＥ１３９４プロトコル等を実行し、出力端子２５を介して他の記録再生装置２に送信する。

【００３２】再生系を構成する暗号解読回路２２は、記憶部１５に記憶されている暗号化されたディジタルデー

タを再生する際に、暗号化回路１３で暗号化されたディジタルデータを解読する。この暗号解読回路２２は、上記図４に示す暗号解読回路１９の構成に加え更に、詳細は省略するが装置共通鍵を記憶する装置共通鍵用メモリ４６と、装置共通鍵生成回路４３からの出力と装置共通鍵用メモリ４６からの出力とを切り換えるセレクタ４７とを有する。

【００３３】セレクタ４７は、サーバ装置３からダウンロードしたディジタルデータを再生するとき、装置共通鍵生成回路４３で生成された装置共通鍵が暗号化鍵解読回路４４に出力されるように切り換え、他の記録再生装置２から専用ケーブルを介して直接的に送信されたディジタルデータを再生するとき、装置共通鍵用メモリ４６に記憶された装置共通鍵が暗号化鍵解読回路４４に出力されるように切り換える。そして、暗号解読回路２２は、暗号解読したディジタルデータをＤ／Ａコンバータ２３に出力する。Ｄ／Ａコンバータ２３は、暗号解読されたディジタルデータをアナログ信号に変換し、スピーカ２４は、このアナログのデータを電気音響変換して出力する。

【００３４】以上のような記録再生装置２において、外部機器から出力されたオーディオデータ等のディジタルデータを記憶部１５に保存する動作について説明すると、外部記憶装置から読み出されたディジタルデータは、入力端子１１から入力され、暗号化回路１３により暗号化される。すなわち、ディジタルデータが暗号化回路１３に入力されると、コンテンツ暗号化回路３７は、コンテンツ鍵用メモリ３３より所定のコンテンツ鍵を読み出し、このコンテンツ鍵を用いてタイトル等のヘッダを除き暗号化する。これと共に、乱数発生回路３１は、乱数を発生し、この乱数を関数回路３２に出力し、関数回路３２は、乱数に基づいて関数を発生する。また、装置共通鍵生成回路３６は、共通鍵用メモリ３４から共通鍵を読み出し、装置個別鍵用メモリ３５から装置固有鍵を読み出し、共通鍵と装置固有鍵とに基づいて装置共通鍵を生成する。コンテンツを暗号化するのに用いるコンテンツ鍵はコンテンツ鍵暗号化回路３８よりコンテンツ鍵暗号化回路３８にも出力され、このコンテンツ鍵暗号化回路３８は、乱数が与えられて関数回路３２で発生された関数と装置共通鍵生成回路３６で生成された装置共通鍵とで、暗号化鍵を生成する。そして、暗号化回路１３は、暗号化されていないヘッダと、乱数発生回路３１で発生された乱数と、共通鍵用メモリ３４から出力された共通鍵と、コンテンツ鍵暗号化回路３８から出力された暗号化鍵と、コンテンツ暗号化回路３７から出力された暗号化コンテンツとからなるパケットを生成する。

【００３５】そして、このパケットは、記録処理回路１４で記録処理がなされた後、記録手段により記憶部１５に記録される。記録再生装置２では、記録部１５に暗号化された状態でディジタルデータが記憶されているが、ヘッダは、暗号化されていない。したがって、記録再生装置２は、記憶部１５に暗号化されているディジタルデータをヘッダを用いることで容易に検索することができ、例えば送信するディジタルデータや再生するディジタルデータを容易に見つけだすことができる。

【００３６】次に、以上のように構成された送信元の記録再生装置２ａがディジタルデータを他の記録再生装置２ｂに送信する際の認証処理を図５を参照して説明する。

【００３７】先ず、ステップＳ１において、利用者によって記憶部１５に記憶されている暗号化されたディジタルデータを送信する送信操作がされると、ステップＳ１において、送信元の記録再生装置２ａの認証回路１８は、送信先の記録再生装置２ｂが同じ規格に準拠した装置であるかどうかの認証を行う。具体的に、記録再生装置２ａは、専用ケーブルを介して又はサーバ装置３を介して送信先の記録再生装置２ｂの認証を行う。そして、送信元の記録再生装置２ａは、送信先の記録再生装置２ｂの認証が取れたときステップＳ２に進み、認証が取れなかったときステップＳ４に進む。

【００３８】ステップＳ２において、送信先の記録再生装置２ａは、ディジタルデータの伝送が専用ケーブルを用いた直接的な伝送であるかサーバ装置３を介した間接的な伝送であるかの判断を行い、送信するディジタルデータの送信方法と通信Ｉ／Ｆ２１の方式を選択する。そして、送信元の記録再生装置２ａは、専用ケーブルを用いた直接的な伝送であるときステップＳ３に進み、サーバ装置３を介した間接的な伝送であるときステップＳ５に進む。

【００３９】ステップＳ３において、専用ケーブルを用いた直接的な伝送であるとき、送信元の記録再生装置２ａは、送信先の記録再生装置２ｂが認証の取れた正規な装置であり、自分の暗号化に対応した暗号解読機能も有する装置であるから、暗号化されたディジタルデータをそのまま専用ケーブルを介して送信先の記録再生装置２ｂに出力する。すなわち、送信元の記録再生装置２ａのセレクタ１７は、図２に示すように、再生処理回路１６と通信Ｉ／Ｆ２１とを直接接続する。これにより、記憶部１５に記憶されている暗号化されたディジタルデータは、再生処理回路１６で再生処理が施された後、そのまま通信Ｉ／Ｆ２１より送信先の記録再生装置２ｂに出力される。したがって、送信元の記録再生装置２ａは、暗号解読や再暗号化処理を行う必要が無いことから高速にディジタルデータを送信先の記録再生装置２に送信することができる。

【００４０】送信先の記録再生装置２ｂには、暗号化されているディジタルデータが入力端子１２より入力され、記録処理回路１４で記録処理がなされた後、記録手段により記憶部１５に記録される。ここで、送信先の記録再生装置２ｂでは、記憶部１５に暗号化されているデ

ィジタルデータが記憶されることになるが、ヘッダは暗号化されていないことから、再生するディジタルデータを容易に検索することができる。そして、記憶部１５に記録されている暗号化されたディジタルデータを再生するとき、再生手段により読み出された暗号化されたディジタルデータは、再生処理回路１６で再生処理が施され、再生系の暗号解読回路２２に出力される。

【００４１】暗号解読回路２２は、図４に示すように、セレクタ４７を、装置共通鍵用メモリ４６に記憶された装置共通鍵を暗号化鍵解読回路４４に出力できるように切り換える。そして、送信元の記録再生装置２ａの暗号化回路１３で暗号化されたディジタルデータが入力されると、関数回路４１は、パケット中の乱数に基づいて関数を発生し、暗号化鍵解読回路４４は、装置共通鍵用メモリ４６に記憶された装置共通鍵を読み出す。暗号化鍵解読回路４４は、関数回路４１で発生された関数と装置共通鍵とによりパケット中より読み出した暗号化鍵を解読し、コンテンツ鍵を生成し、コンテンツ解読回路４５に出力する。コンテンツ解読回路４５は、パケット中より暗号化コンテンツを読み出し、これをコンテンツ鍵を用いて解読する。なお、パケット中のヘッダは、暗号化されていないので暗号解読回路２２は、そのままパケット中より読み出す。そして、暗号解読回路２２は、暗号解読したディジタルデータをＤ／Ａコンバータ２３に出力する。Ｄ／Ａコンバータ２３は、暗号解読されたディジタルデータをアナログ信号に変換し、スピーカ２４は、このアナログのデータを電気音響変換して出力する。

【００４２】また、ステップＳ１において、送信元の記録再生装置２ａは、送信先の記録再生装置２ｂの認証が取れなかったときも、ステップＳ４において、暗号化されたディジタルデータをそのまま専用ケーブルを介して又はサーバ装置３を介して送信先の記録再生装置２ｂに出力する。すなわち、送信先の記録再生装置２ａは、図２に示すように、セレクタ１７を切り換え再生処理回路１６と通信Ｉ／Ｆ２１とを直接接続する。これにより、記憶部１５に記憶されている暗号化されたディジタルデータは、再生処理回路１６で再生処理が施された後、そのまま通信Ｉ／Ｆ２１より送信先の記録再生装置２ｂに出力される。送信先の記録再生装置２ｂには、暗号化されているディジタルデータが入力端子１２より入力され、記録処理回路１４で記録処理がなされた後、記録手段により記憶部１５に記録される。

【００４３】ここで、送信先の記録再生装置２ｂは、認証が取れなかった装置であり、暗号解読機能を有していないことから、暗号化されたディジタルデータを解読することはできない。したがって、正規な利用者でない者に仮にディジタルデータが渡ったとしても、このディジタルデータが再生されることを防止することができる。

【００４４】また、ステップＳ２において、送信元の記録再生装置２ａは、サーバ装置３を介した間接的な伝送であると判断したとき、ステップＳ５において、記憶部１５に記録されている暗号化されたディジタルデータは、再生手段により読み出された後、再生処理回路１６で再生処理が施される。ここで、セレクタ１７は、再暗号化をすることができるように再生処理回路１６と暗号解読回路１９とを接続する。

【００４５】そして、暗号解読回路１９に暗号化されたディジタルデータが入力されると、図４に示すように、関数回路４１は、パケット中の乱数に基づいて関数を発生し、装置共通鍵生成回路４３は、パケット中の共通鍵と装置個別鍵用メモリ４２より装置個別鍵とを読み出し、装置共通鍵を生成し、暗号化鍵解読回路４４に出力する。暗号化鍵解読回路４４は、関数回路４１で発生された関数と装置共通鍵とによりパケット中より読み出した暗号化鍵を解読し、コンテンツ鍵を生成し、コンテンツ解読回路４５に出力する。コンテンツ解読回路４５は、パケット中より暗号化コンテンツを読み出し、これをコンテンツ鍵を用いて解読する。なお、パケット中のヘッダは、暗号化されていないので、暗号解読回路１９は、そのままパケット中より読み出す。そして、暗号解読回路１９は、暗号解読後のディジタルデータを再暗号化回路２０に出力する。

【００４６】次いで、ステップＳ６において、送信元の記録再生装置２ａは、認証が取れた送信先の記録再生装置２ｂで暗号解読ができるように、送信先の記録再生装置２ｂの装置個別鍵用メモリ３５から装置個別鍵をサーバ装置３を介して取得する。

【００４７】次いで、ステップＳ７において、送信元の記録再生装置２ａは、暗号解読回路１９で暗号解読されたディジタルデータに対して再度ステップＳ６で取得した装置個別鍵を用いて再暗号化回路２０で再暗号化を行う。すなわち、ディジタルデータが再暗号化回路２０に入力されると、コンテンツ暗号化回路３７は、コンテンツ鍵用メモリ３３より所定のコンテンツ鍵を読み出し、このコンテンツ鍵を用いてタイトル等のヘッダを除き暗号化する。これと共に、乱数発生回路３１は、乱数を発生し、この乱数を関数回路３２に出力し、関数回路３２は、乱数に基づいて関数を発生する。また、装置共通鍵生成回路３６は、共通鍵用メモリ３４から共通鍵を読み出した共通鍵と送信先の記録再生装置２ｂから取得した装置固有鍵とに基づいて装置共通鍵を生成する。コンテンツを暗号化するのに用いるコンテンツ鍵はコンテンツ鍵暗号化回路３８よりコンテンツ鍵暗号化回路３８にも出力され、このコンテンツ鍵暗号化回路３８は、乱数が与えられて関数回路３２で発生された関数と装置共通鍵生成回路３６で生成された装置共通鍵とで、暗号化鍵を生成する。そして、再暗号化回路２０は、暗号化されていないヘッダと、乱数発生回路３１で発生された乱数と、共通鍵用メモリ３４から出力された共通鍵と、コン

テンツ鍵暗号化回路３８から出力された暗号化鍵と、コンテンツ暗号化回路３７から出力された暗号化コンテンツとからなるパケットを生成し、通信Ｉ／Ｆ２１に出力する。

【００４８】かくして、再暗号化がされたディジタルデータは、ネットワーク５を介してサーバ装置３に送信され、一時的に保存される。このとき、権限を有しない端末装置がサーバ装置３にアクセスし、記録再生装置２ａが送信したディジタルデータをダウンロードし記憶部に保存したときであっても、この端末装置は、暗号を解読することができない。したがって、サーバ装置３に一時的に記録されているディジタルデータは、権限の有しない利用者の端末装置で再生されることを防止することができる。また、サーバ装置３に多くの暗号化されたディジタルデータが保存されているときにも、ヘッダが暗号化されていないことから、記録再生装置２ａ，２ｂからサーバ装置３のデータを容易に検索することができる。

【００４９】送信先の記録再生装置２ｂは、サーバ装置３にアクセスすることによって、自分宛のディジタルデータをダウンロードすることができる。ダウンロードした暗号化されているディジタルデータは、入力端子１２より入力され、記録処理回路１４で記録処理がなされた後、記録手段により記憶部１５に記録される。ここで、送信先の記録再生装置２ｂでは、記憶部１５に暗号化されているディジタルデータが記憶されることになるが、ヘッダは暗号化されていないことから、再生するディジタルデータを容易に検索することができる。記憶部１５に記録されている暗号化されたディジタルデータを再生するときには、再生手段により読み出された後、再生処理回路１６で再生処理が施されると、再生系の暗号解読回路２２に出力される。

【００５０】ここで、図４に示すように、セレクタ４７は、装置共通鍵生成回路４３で生成された装置共通鍵が暗号化鍵解読回路４４に出力されるように切り換える。そして、暗号化回路１３に暗号化されたディジタルデータが入力されると、関数回路４１は、パケット中の乱数に基づいて関数を発生し、装置共通鍵生成回路４３は、パケット中の共通鍵と装置個別鍵用メモリ４２より装置個別鍵とを読み出し、装置共通鍵を生成し、暗号化鍵解読回路４４に出力する。ここで、記録再生装置２ｂの装置個別鍵用メモリ４２の装置個別鍵は、送信元の記録再生装置２がステップＳ６で取得したものと同じである。暗号化鍵解読回路４４は、関数回路４１で発生された関数と装置共通鍵とによりパケット中より読み出した暗号化鍵を解読し、コンテンツ鍵を生成し、コンテンツ解読回路４５に出力する。コンテンツ解読回路４５は、パケット中より暗号化コンテンツを読み出し、これをコンテンツ鍵を用いて解読する。なお、パケット中のヘッダは、暗号化されていないので暗号解読回路２２は、そのままパケット中より読み出す。そして、暗号解読回路２２は、暗号解読したディジタルデータをＤ／Ａコンバータ２３に出力する。Ｄ／Ａコンバータ２３は、暗号解読されたディジタルデータをアナログ信号に変換し、スピーカ２４は、このアナログのデータを電気音響変換して出力する。

【００５１】以上のようなシステムでは、サーバ装置３に一時的に保存されているディジタルデータを権限を有しない記録再生装置がダウンロードし記憶部に保存することはあっても、このディジタルデータは、暗号化されていることから、権限を有しない記録再生装置で再生されることな無い。したがって、このシステムでは、ディジタルデータ中に無断複写防止情報を入れること無く著作権管理を行うことができる。

【００５２】なお、以上、記録再生装置２ａ，２ｂ間でディジタルデータの伝送を行うとき専用ケーブルを用いる場合を例に取り説明したが、無線で行うようにしてもよい。

【００５３】次に、ディジタルデータを本システムの専用機器である記録再生装置２ａと記録再生装置２ｂとの間でやり取りする他の例を説明する。記録再生装置２ａ，２ｂは、有線又は無線で直接的にデータをやり取りし、また、本システムに使用する専用機器である。したがって、ディジタルデータの通信を行うに際しては、安全な環境である。そこで、送信元の記録再生装置２ａは、送信先の記録再生装置２ｂの認証が取れたとき、暗号化されているディジタルデータをそのまま記録再生装置２ｂに送信するようにし、認証が取れなかったとき、ディジタルデータの出力を禁止するようにする。また、本例では、データ通信の際の安全性を高めるため、上述の例のように、権限の無い装置がアクセス可能なサーバ装置３を介してディジタルデータをやり取りはしないようにしている。以下、この例を、図６及び図７を参照して説明する。

【００５４】図６に示すように、この記録再生装置５０は、図２に示す記録再生装置２と送信系を除き同様の構成を有するものであり、他の記録再生装置２にディジタルデータを送信するための送信系として、データの送信先の装置の認証を行う認証回路５１と、認証回路５１で送信先の装置の認証が取れたときに限ってデータの出力を可能とするセレクタ５２とを備える。

【００５５】認証回路５１は、送信先の装置の認証を取り、認証結果に基づいてセレクタ５２を切換制御する。すなわち、認証回路５１は、送信先の装置が専用機器である記録再生装置５０であるとき、暗号化されたディジタルデータの送信が可能であるとして、再生処理回路１６と通信Ｉ／Ｆ２１とを接続するようにセレクタ５２を切り換える。また、認証回路５１は、送信する装置がサーバ装置３であったり、汎用機器であるパーソナルコンピュータ等であったりして記録再生装置５０でないとき、暗号化されたディジタルデータの出力を禁止するた

め、再生処理回路１６と通信Ｉ／Ｆ５３を接続しないようにセレクタ５２を切り換える。

【００５６】次に、図７を用いて、記録再生装置５０がディジタルデータを他の装置に送信する際の手順について説明する。先ずステップＳ１１において、利用者によって記憶部１５に記憶されている暗号化されたディジタルデータを送信する送信操作がされると、送信元の記録再生装置５０の認証回路５１は、送信先の装置が記録再生装置５０で有るかどうかを判断する。すなわち、認証回路５１は、送信先の装置が、直接的にパーソナルコンピュータ等の汎用機器であったり、送信先が記録再生装置５０であっても直接的にはサーバ装置３であったりした場合、送信先の装置を認証しないようにする。サーバ装置３に送信する場合には、権限の無い装置に不正にダウンロードされるおそれがあり、必ずしも安全な環境であるといえず、汎用機器であるパーソナルコンピュータに送信する場合には、暗号を解読するソフトウェアがパーソナルコンピュータに不正にインストールされており、暗号化されたディジタルデータが不正に解読されてしまうおそれがあるためである。そこで、記録再生装置５０では、専用機器である記録再生装置５０が直接接続されるときに限って、ディジタルデータの送信をできるようにしている。

【００５７】そして、認証回路５１は、記録再生装置５０に直接的にディジタルデータを送信するとき、ステップＳ１２において、セレクタ５２を、再生処理回路１６と通信Ｉ／Ｆ２１とを接続するように切り換える。そして、記録再生装置５０は、送信先の記録再生装置５０に暗号化されているディジタルデータを送信する。

【００５８】また、認証回路５１は、送信先の装置が、直接的にパーソナルコンピュータ等の汎用機器であったり、送信先が記録再生装置５０であっても直接的にはサーバ装置３であったりするとき、ステップＳ１３において、再生処理回路１６と通信Ｉ／Ｆ２１との接続をオフにする。すなわち、記録再生装置５０は、送信先の装置への暗号化されたディジタルデータの出力を禁止する。

【００５９】以上のような記録再生装置５０は、完全に安全な環境でディジタルデータを送信することができる場合、すなわち記録再生装置５０へ直接的に出力する場合に限って、暗号化されたディジタルデータの出力を許可することで、安全にディジタルデータの送受信を行うことができる。また、ディジタルデータの送信を行うとき、記憶部１５に暗号化された状態で保存されているディジタルデータは、再暗号化をすることなく送信先の記録再生装置５０に送信されるから、再暗号化のための時間を省くことができる。

【００６０】なお、以上の例では、送信先の装置が記録再生装置５０である場合に限ってディジタルデータを出力することができる場合を説明したが、送信先の装置は、安全な環境でディジタルデータの出力することができる装置であれば記録再生装置５０に限定されるものではない。例えば、本システムに準拠した暗号解読回路等が専用の半導体チップ等で構成された装置が送信先の装置であるときには、信用できる装置であり安全にデータのやり取りが行うことができることから、ディジタルデータの出力を許可するようにしてもよい。

【００６１】次に、ディジタルデータを本システムの専用機器である記録再生装置の他に汎用機器であるパーソナルコンピュータ等にも認証が取れた場合に出力することができる例を図８及び図９を参照して説明する。

【００６２】図８に示すように、この記録再生装置６０は、送信系を除き、図２に示す記録再生装置２と同様な構成を有するものであり、暗号化されたディジタルデータを他の装置に送信する送信系として、送信先の装置が本システムの専用機器である記録再生装置６０であるかの認証を行う第１の認証回路６１と、暗号化されたディジタルデータをそのまま出力する経路と暗号化されたディジタルデータを再暗号化して出力する経路とを切り換える第１のセレクタ６２と、送信先の装置がパーソナルコンピュータ等の汎用機器であるかの認証を行う第２の認証回路６３と、第２の認証回路６３で汎用機器の認証が取れたとき暗号化されたディジタルデータの出力を許可する第２のセレクタ６４と、暗号化されたディジタルデータを解読する暗号解読回路６５と、暗号解読回路６５で暗号解読されたディジタルデータを再暗号化する再暗号化回路６６とを備える。

【００６３】第１の認証回路６１は、送信先の装置の認証を取り、認証結果に基づいてセレクタ５２を切換制御する。すなわち、第１の認証回路６１は、送信先の装置が専用機器である記録再生装置６０であり、この記録再生装置６０に直接的にディジタルデータを送信するとき、暗号化されたディジタルデータの送信が可能であるとして、再生処理回路１６と通信Ｉ／Ｆ２１とを接続するように第１のセレクタ６２を切り換える。また、第１の認証回路６１は、記録再生装置６０であってもサーバ装置３を介して送信する場合や直接的にディジタルデータを送信する場合であってもパーソナルコンピュータ等の汎用機器に送信する場合、再生処理回路１６と通信Ｉ／Ｆ２１とを切断し、再生処理回路１６と第２のセレクタ６４とを接続するように切り換える。

【００６４】第２の認証回路６３は、送信先がパーソナルコンピュータ等の汎用機器で暗号解読のためのソフトウェアが正規にインストールされた装置であるか、又は、サーバ装置３を介して記録再生装置６０や汎用機器に送信する際の記録再生装置６０や汎用機器の認証を行い、認証結果に基づいて第２のセレクタ６４を切換制御する。すなわち、第２の認証回路６３は、暗号解読のためのソフトウェアが正規にインストールされた汎用機器に暗号化されたディジタルデータを送信する場合や、サーバ装置３を介して記録再生装置６０に暗号化されたデ

ィジタルデータを送信する場合や、サーバ装置３を介して正規にソフトウェアがインストールされた汎用機器に暗号化されたディジタルデータを送信する場合に、第１のセレクタ６２を介して再生処理回路１６と暗号解読回路６５とを接続するオンの状態に第２のセレクタ６４を切り換える。また、第２の認証回路６３は、送信先の装置の認証が取れなかったとき、第２のセレクタ６４を、再生処理回路１６と暗号解読回路６５とを接続しないオフの状態に切り換える。第２の認証回路６３は、ディジタルデータの出力禁止の状態にする。

【００６５】暗号解読回路６５は、ディジタルデータを送信する際、再暗号化するため上述した暗号化回路１３で暗号化されたディジタルデータを解読し、再暗号化回路６６に出力する。

【００６６】再暗号化回路６６は、第２の認証回路６３で認証が取れた汎用機器より公開鍵を取得し、この公開鍵を用いてディジタルデータを再暗号化する。そして、再暗号化回路６６は、再暗号化されたディジタルデータを通信Ｉ／Ｆ２１に出力する。

【００６７】次に、図９を用いて、記録再生装置６０がディジタルデータを他の装置に送信する際の手順について説明する。利用者によって記憶部１５に記憶されている暗号化されたディジタルデータを送信する送信操作がされると、送信元の記録再生装置６０の第１の認証回路６１は、ステップＳ２１において、送信先の装置が記録再生装置６０で有るかどうかを判断する。すなわち、第１の認証回路６１は、直接的に記録再生装置６０にディジタルデータを送信するのか、記録再生装置６０以外の装置にディジタルデータを送信するのかを判断する。

【００６８】送信先の装置が記録再生装置６０であると認証が取れたとき、第１の認証回路６１は、ステップＳ２２において、再生処理回路１６から通信Ｉ／Ｆ２１にディジタルデータを出力することができるように第１のセレクタ６２を切り換える。これによって、記憶部１５より読み出された暗号化されたディジタルデータは、暗号化されたままの状態で通信Ｉ／Ｆ２１より送信先の記録再生装置６０に送信される。この場合、記録再生装置６０は、再暗号化を行わないことから、高速にディジタルデータを送信することができる。送信先の記録再生装置６０は、このディジタルデータを再生する場合、共通鍵を用いて暗号を解読し再生する。

【００６９】ステップＳ２１において第１の認証回路６１が送信先の装置を認証しなかったとき、ステップＳ２３において、第２の認証回路６３は、送信先の装置の認証を行う。すなわち、第２の認証回路６３は、直接又はサーバ装置３を介して接続された装置が暗号解読のためのソフトウェアが正規にインストールされた汎用機器であるかどうか、サーバ装置３を介して接続された装置が記録再生装置６０であるときかどうかの判断を行う。

【００７０】そして、第２の認証回路６３で送信先の装置の認証が取れたとき、ステップＳ２４において、第２の認証回路６３は、第１のセレクタ６２を介して再生処理回路１６と暗号解読回路６５とを接続するオンの状態に第２のセレクタ６４を切り換える。そして、記憶部１５から読み出された暗号化されているディジタルデータは、暗号解読回路６５に入力される。そして、暗号解読回路６５は、再暗号化するため上述した暗号化回路１３で暗号化されたディジタルデータを解読し、再暗号化回路６６に出力する。

【００７１】再暗号化回路６６は、ステップＳ２５において、送信先の装置の公開鍵を取得する。ステップＳ２６において、再暗号化回路６６は、暗号解読回路６２で暗号解読されたディジタルデータを再度暗号化する。そして、通信Ｉ／Ｆ２０は、この再暗号化されたディジタルデータを送信先の装置に送信する。すなわち、ステップＳ２３で送信先の装置が汎用機器であったり、サーバ装置３に送信する場合は、ステップＳ２２の場合に比べ安全性が低いため、送信先の装置の公開鍵を用いて再暗号化してディジタルデータを送信するようにして安全性を維持するようにしている。

【００７２】また、ステップＳ２７において、送信先の装置の認証が取れなかったとき、送信先の装置は、正規な装置ではないことから、第２の認証回路６３は、再生処理回路１６と通信Ｉ／Ｆ２１との接続をオフにする。すなわち、記録再生装置５０は、送信先の装置への暗号化されたディジタルデータの出力を禁止する。

【００７３】以上のような記録再生装置６０は、完全に安全な環境でディジタルデータを送信することができる場合、すなわち記録再生装置６０へ直接的に出力する場合に限って、暗号化されたディジタルデータの出力を許可することで、安全にディジタルデータの送受信を行うことができる。このとき、記憶部１５に暗号化された状態で保存されているディジタルデータは、再暗号化をすることなく送信先の記録再生装置５０に送信されるから、送信先の記録再生装置５０は、ディジタルデータを高速に出力することができる。また、記録再生装置６０への直接的な出力でない場合であっても、送信先の機器の認証が取れたときには、再暗号化をすることで、安全性を確保しつつディジタルデータを他の装置に送信することができる。すなわち、本例では、図６及び図７の例よりも出力することができる装置の種類を増やすことができる。

【００７４】次に、出力先の装置の特徴に応じて出力方法を変えることができる記録再生装置７０の例を図１０及び図１１を参照して説明する。この記録再生装置７０は、図２に示す記録再生装置２と送信系を除きほぼ同様な構成を有する装置であり、暗号化されたディジタルデータを他の装置に送信する送信系として、送信先の装置の認証を取る認証回路７１と、認証回路７１での認証結果に応じて送信先の装置の種類を判別する判別回路７２

と、再生処理回路１６から出力された暗号化されたディジタルデータの暗号を解読する暗号解読回路７３と、暗号解読回路７３で暗号解読されたディジタルデータを再暗号化する再暗号化回路７４とを備える。また、記録再生装置７０は、アナログ出力として、再生処理回路１６から出力されたディジタルデータの暗号を解読する暗号解読回路７５と、暗号解読されたディジタルデータをアナログデータに変換するＤ／Ａコンバータ７６とを備える。

【００７５】認証回路７１は、送信先の装置の認証を行う。具体的に、認証回路７１は、送信先の装置が本システムの専用機器である記録再生装置７０であるか、本システムを利用するためのソフトウェアが正規にインストールされたパーソナルコンピュータ等の汎用機器であるか、サーバ装置３を介して接続された記録再生装置６０若しくは汎用機器であるか等送信先の装置が正当な権限を有しているかどうかの認証を行う。そして、認証回路７１は、認証の取れた装置の種類と認証結果を判別回路７２に出力する。

【００７６】判別回路７２は、認証回路７１からの出力に応じて、暗号化されたディジタルデータを送信する送信先の装置の種類を判別する。そして、判別回路７２は、ディジタルデータを直接的に認証の取れた記録再生装置７０に送信するとき、再生処理回路１６と通信Ｉ／Ｆ２０とを接続するようにする。また、判別回路７２は、ディジタルデータを直接的に汎用機器に送信するときや、間接的、すなわちサーバ装置３を介して記録再生装置７０や汎用機器に送信するとき、再生処理回路１６と暗号解読回路７３とを接続するようにする。更に、判別回路７２は、ディジタルデータの送信する装置が正当な権限を有していない、すなわち認証できなかったとき、ディジタルデータの出力を禁止するか、アナログ出力をするため暗号解読回路７５とを接続するようにする。

【００７７】暗号解読回路７３は、ディジタルデータを送信する際、再暗号化するため上述した暗号化回路１３で暗号化されたディジタルデータを解読し、再暗号化回路７５に出力する。

【００７８】再暗号化回路７４は、認証回路７１で認証が取れた記録再生装置や汎用機器より公開鍵を取得し、この公開鍵を用いてディジタルデータを再暗号化する。そして、再暗号化回路７４は、再暗号化されたディジタルデータを通信Ｉ／Ｆ２１に出力する。

【００７９】また、暗号解読回路７５は、アナログ出力するため上述した暗号化回路１３で暗号化されたディジタルデータを解読し、Ｄ／Ａコンバータ７６に出力する。そして、Ｄ／Ａコンバータ７６は、ディジタルデータをアナログデータに変換し、アナログデータを出力する。

【００８０】次に、図９を用いて、記録再生装置６０がディジタルデータを他の装置に送信する際の手順について説明する。利用者によって記憶部１５に記憶されている暗号化されたディジタルデータを送信する送信操作がされると、送信元の記録再生装置７０の認証回路７１は、ステップＳ３１において、ディジタルデータの送信先の装置が権限を有する装置であるかの認証を行い、認証結果と認証が取れた装置の種類とを、判別回路７２に出力する。判別回路７２は、認証結果に応じて、再生処理回路１６からの暗号化されているディジタルデータを、通信Ｉ／Ｆ２０に出力するか、暗号化回路７３に出力するか、出力禁止若しくは暗号解読回路７５に出力するかを判断する。

【００８１】判別回路７２は、送信先の記録再生装置７０に直接的にディジタルデータを送信すると判断したとき、ステップＳ３２において、再生処理回路１６から出力された暗号化されているディジタルデータを通信Ｉ／Ｆ２１に出力する。この場合、記憶部１５より読み出された暗号化されたディジタルデータは、通信環境が安全な状態で行われることから、暗号化されたままの状態で通信Ｉ／Ｆ２１より送信先の記録再生装置６０に送信される。そして、記録再生装置７０は、ディジタルデータを送信する際、再暗号化を行わないことから、高速にディジタルデータを送信することができる。送信先の記録再生装置６０は、このディジタルデータを再生する場合、共通鍵を用いて暗号を解読し再生する。

【００８２】判別回路７２は、送信先の装置である送信元の装置に直接的に接続された汎用機器やサーバ装置３を介して記録再生装置７０若しくは汎用機器にディジタルデータを送信すると判断したとき、ステップＳ３３において、再生処理回路１６と暗号解読回路７３とを接続する。そして、暗号解読回路７３は、再暗号化するため上述した暗号化回路１３で暗号化されたディジタルデータを解読し、再暗号化回路７４に出力する。ステップＳ３４において、再暗号化回路７４は、送信先の装置の公開鍵を取得する。ステップＳ３５において、再暗号化回路７４は、暗号解読回路７３で暗号解読されたディジタルデータを取得した公開鍵を用いて再度暗号化する。そして、通信Ｉ／Ｆ２０は、この再暗号化されたディジタルデータを送信先の装置に送信する。すなわち、送信先の装置が汎用機器であったり、サーバ装置３に送信する場合は、ステップＳ３２の場合に比べ安全性が低いため、送信先の装置の公開鍵を用いて再暗号化してディジタルデータを送信するようにして安全性を維持するようにしている。

【００８３】判別回路７２は、ステップＳ３６において、ディジタルデータの送信先の装置が権限を有していない装置であると判断したとき、ステップＳ３６において、ディジタルデータの出力を禁止する。又は、判別回路７２は、ステップＳ３６において、アナログ出力に限って許可する。アナログ出力を行う場合、判別回路７２

は、再生処理回路１６と暗号解読回路７５とを接続する。そして、暗号解読回路７５は、再暗号化するため上述した暗号化回路１３で暗号化されたディジタルデータを解読し、Ｄ／Ａコンバータ７６に出力する。

【００８４】以上のような記録再生装置７０では、送信先の装置の種類に応じて、安全度を変えて出力することができる。すなわち、直接的に記録再生装置７０にディジタルデータを送信する場合は、専用機器間のデータ伝送であるから安全度が高い。したがって、記録再生装置７０は、送信時間を短くするため、再暗号化をすること無く、記憶部５１に暗号化されているディジタルデータをそのまま送信先の記録再生装置７０に送信するようにしている。また、本システムで使用する暗号解読等のソフトウェアがインストールされたパーソナルコンピュータ等の汎用機器は、不正にソフトウェアがインストールされた場合等が想定され、安全度が専用機器間でのデータ伝送に比べ低い。また、サーバ装置３を介して記録再生装置７０や汎用機器にディジタルデータを送信する場合にも、不正にサーバ装置３にアクセスした装置がダウンロードするおそれがあり安全度が専用機器間での伝送より低くなる。そこで、記録再生装置７０は、このような場合、送信先の公開鍵を用いて再暗号化を行い、安全度を維持するようにしている。

【００８５】なお、以上、ディジタルデータを暗号化してデータを送信する場合を説明したが、暗号の具体的方法としては、公開鍵暗号方式としてＲＳＡ暗号、だ円暗号等を、また、公開鍵方式より暗号化速度の速い秘密鍵方式として、ＥＫＢやＭＪＲを用いるようにしてもよい。例えば、専用機器間では、暗号加速度の速い公開鍵方式を用い、汎用機器へのデータ伝送やサーバ装置３を介してのデータ伝送では、安全度の高い公開鍵方式を用いるとよい。

【００８６】次に、記録再生装置２に送信されてきたディジタルデータに著作権管理データとしてディジタルデータの複写を制限する無断複写防止情報が含まれているときに、この無断複製防止情報に基づいて、ディジタルデータの記録を制限する記録再生装置２について図面を参照して説明する。

【００８７】この記録再生装置８０は、図１２に示すように、サーバ装置３から暗号化され圧縮されたディジタルデータが入力される入力端子８１を有する。また、この記録再生装置８０は、記録系として、暗号化されたディジタルデータを解読する暗号解読回路８２と、圧縮されているディジタルデータを伸長する伸長回路８３と、ディジタルデータの中から無断複写防止情報を抽出し書き換える抽出更新回路８４と、ディジタルデータを圧縮する圧縮回路８５と、圧縮されているディジタルデータを暗号化する暗号化回路８６と、暗号化されたディジタルデータに記録処理を施す記録処理回路８７と、暗号化されたディジタルデータを保存する記憶部８８とを有する。

【００８８】また、記録再生装置８０は、再生系として、再生処理回路８９と、暗号化されて記憶部８８に記憶されているディジタルデータを解読する暗号解読回路９０と、圧縮されているディジタルデータを伸長する伸長回路９１と、ディジタル信号をアナログ信号に変換するＤ／Ａコンバータ９２と、アナログ信号を出力するアナログ出力端子９３と、Ｄ／Ａコンバータ９２の前段のディジタルデータを出力するディジタル出力端子９４とを有する。また、記録再生装置８０は、全体の動作を制御するシステムコントローラ９５を有する。

【００８９】入力端子８１には、サーバ装置３や他の記録再生装置２から暗号化され圧縮されたされたオーディオデータ、ビデオデータ、画像データ等のディジタルデータが入力される。また、このディジタルデータには、ＳＣＭＳ（Serial Copy Management System）情報がウォータマークで記録されている。暗号解読回路８２は、入力端子８１から入力された暗号化されたディジタルデータを解読し、ディジタルデータに含まれる無断複写防止情報を抽出できるようにし、伸長回路８３に出力する。伸長回路８３は、ＡＴＲＡＣ３（Adaptive Transform Acoustic Coding 3：商標）、ＭＰＥＧ－２ＡＡＣ（Motion Picture Expert Group 2 AdvancedAudio Coding：商標）、ＭＰ３（MPEG-1 Audio Layer3：商標）、ＴｗｉｎＶＱ（Transform-Domain Weighted Interleave Vector Quantization：商標）、ＭＳＡｕｄｉｏ（WMA:Windows Media Audio：商標）、Ｏｇｇ　Ｖｏｒｂｉｓ（商標）等の方式で圧縮されているディジタルデータを伸長し、抽出更新回路８４に出力する。

【００９０】抽出更新回路８４は、暗号解読がされデータが伸長されたディジタルデータ中に含まれるウォータマークを検出し、ＳＣＭＳ情報を抽出する。このＳＣＭＳ情報は、データの先頭の２ビットに設けられるの複写禁止フラグであり、データの先頭２ビットには「００」（ディジタル複写許可）、「１０」（ディジタル複写禁止）、「１１」（一度だけディジタル複写を認める）の何れかからなる。

【００９１】そして、抽出更新回路８４は、ＳＣＭＳ情報が「００」、「１１」であるとき、記憶部８８にディジタルデータを記録することを許可する。また、ＳＣＭＳ情報が「１１」のときには、「１１」を「１０」に書き換える。また、抽出更新回路８４は、ＳＣＭＳ情報が「１０」であるとき、記憶部８８へのディジタルデータの記録を禁止する。そして、抽出更新回路８４は、ＳＣＭＳ情報が更新されたディジタルデータを圧縮回路８５に出力する。

【００９２】なお、ＳＣＭＳ情報は、ＣＧＭＳ（Copy Generation Management System）であってもよい。この場合、ディジタルデータ中には、「１１」（ディジタル複写は一切認めない）、「１０」（これ以上のディジタ

ル複写は認めない）、「０１」（一度だけのディジタル複写は認める）、「００」（自由にディジタル複写を認める）の２ビットからなるＣＣＩ（Copy Control Information）が埋め込まれる。勿論、無断複写防止情報としては、ＳＣＭＳやＣＧＭＳに限定されるものではない。

【００９３】圧縮回路８５は、ディジタルデータを上述したＡＴＲＡＣ３、ＭＰＥＧ－２ＡＡＣ、ＭＰ３、ＴｗｉｎＶＱ、ＭＳ　Ａｕｄｉｏ、Ｏｇｇ　Ｖｏｒｂｉｓ等の方式で圧縮し、記録処理回路８７に出力する。記録処理回路８７は、例えば入力されたデータにエラー訂正符号化処理や変調処理を施し２値化する。そして、記録処理が施されたデータは、磁気ヘッドや光ピックアップ等の記録手段によってハードディスク、記録可能な光ディスク、光磁気ディスク等からなる記憶部８８を構成する記録媒体に記録される。なお、記憶部８８は、装置本体に内蔵されたものであってもよく、装置本体に対して着脱可能であってもよい。

【００９４】また、記憶部８８に記憶されているデータは、磁気ヘッドや光ピックアップ等の再生手段によって記録媒体から読み出され再生処理回路８９に出力される。再生処理回路８９は、再生手段から出力を２値化し、復調処理やエラー訂正処理を施して暗号解読回路９０に出力する。暗号解読回路９０は、暗号化されているディジタルデータを再生できるように、暗号化回路８６で暗号化されたディジタルデータを解読し、伸長回路９１に出力する。

【００９５】伸長回路９１は、ＡＴＲＡＣ３、ＭＰＥＧ－２ＡＡＣ、ＭＰ３、ＴｗｉｎＶＱ、ＭＳ　Ａｕｄｉｏ、Ｏｇｇ　Ｖｏｒｂｉｓ等の方式で圧縮回路８５で圧縮されたディジタルデータを伸長し、Ｄ／Ａコンバータ９２又はディジタル出力端子９４に出力する。Ｄ／Ａコンバータ９２は、暗号解読されたディジタルデータをアナログ信号に変換し、アナログ出力端子９３に出力する。アナログ出力端子９３は、例えばスピーカが接続されており、アナログ信号に変換されたデータは、電気音響変換されてスピーカより出力される。

【００９６】システムコントローラ９５は、装置全体を制御するものである。例えば、システムコントローラ９５は、入力されたディジタルデータのＳＣＭＳ情報が「００」、「１１」であるとき、記憶部８８にディジタルデータを記録することを許可するように記録処理回路８７を制御し、また、ＳＣＭＳ情報が「１０」であるとき、記憶部８８へのディジタルデータの記録を禁止するように記録処理回路８７を制御する。また、システムコントローラ９５は、ＳＣＭＳ情報が「１１」のとき、「１１」を「１０」に書き換えるように抽出更新回路８４を制御する。

【００９７】以上のような記録再生装置８０を用いるシステムでは、先ず、送信元の記録再生装置８０ａより所定の方式で暗号化され暗号化されたオーディオデータ等のディジタルデータがサーバ装置３にアップロードされる。この暗号化されたディジタルデータには、上述したＳＣＭＳ情報が含まれている。ここで、アップロードするディジタルデータが自由にディジタル複写を認めるデータであるとき、ＳＣＭＳ情報は、「００」とされ、一度だけディジタル複写を認めるデータであるとき、ＳＣＭＳ情報は、「１１」とされ、ディジタル複写を禁止するものであるとき、ＳＣＭＳ情報は、「１０」とされる。サーバ装置３は、送信元の記録再生装置８０ａからの暗号化されたディジタルデータを受信すると、一時的に、ハードディスク等から構成される記憶部にそのまま記憶する。すなわち、サーバ装置３は、暗号化されたディジタルデータを解読し再生する機能を有していない。したがって、サーバ装置３は、将来的にも記憶部に記憶したディジタルデータを解読し再生する可能性を有していないことから、ＳＣＭＳ情報を更新しない。

【００９８】そして、図１３に示すように、送信先の記録再生装置８０ｂは、サーバ装置３にアクセスすることによって、サーバ装置３に蓄積されているディジタルデータをダウンロードする。すると、ダウンロードされたディジタルデータは、暗号解読回路８２に入力される。ここで、システムコントローラ９５は、ステップＳ４１で、ダウンロードしたディジタルデータを暗号解読回路８２で解読できるかどうかを判断する。そして、システムコントローラ９５は、解読できるとき、ステップＳ４２に進み、解読できないとき、ステップＳ４６に進む。

【００９９】暗号解読回路８２は、ダウンロードしたディジタルデータを解読すると、伸長回路８３に出力し、伸長回路８３は、圧縮されたディジタルデータを伸長し、抽出更新回路８４に出力する。抽出更新回路８４は、ＳＣＭＳ情報が記録されたウォータマークを抽出し、システムコントローラ９５にＳＣＭＳ情報を入力する。システムコントローラ９５は、ステップＳ４２において、ＳＣＭＳ情報が「００」、「１１」、「１０」の何れであるかを判断する。

【０１００】ステップＳ４２におけるＳＣＭＳ情報の読出結果に基づいて、システムコントローラ９５は、ステップＳ４３において、ＳＣＭＳ情報が「００」であるとき、記憶部８８にディジタルデータを記録することを許可するように記録処理回路８７を制御する。

【０１０１】また、ステップＳ４４において、システムコントローラ９５は、ＳＣＭＳ情報が「０１」であるとき、記憶部８８にディジタルデータを記録することを許可するように記録処理回路８７を制御すると共に、「１１」を「１０」に書き換えるように抽出更新回路８４を制御する。そして、抽出更新回路８４は、システムコントローラ９５からのコマンドに基づいてＳＣＭＳ情報を「１１」から「１０」に書き換える。

【０１０２】そして、ステップＳ４３及びステップＳ４４において記憶部８８への記録が許可されると、抽出更

新回路８４は、圧縮回路８５に出力し、圧縮回路８５は、再度ディジタルデータを圧縮し暗号化回路８６に出力し、暗号化回路８６は、再度所定の方式で暗号化し記録処理回路８７に出力する。記録処理回路８７は、記録に必要な処理を施し、記録手段に出力する。そして、記録手段は、記憶部８８を構成する記録媒体に暗号圧縮されたディジタルデータを記録する。

【０１０３】また、ステップＳ４５において、システムコントローラ９５は、ＳＣＭＳ情報が「１０」であるとき、記憶部８８にディジタルデータを記録することを禁止するように記録処理回路８７を制御する。システムコントローラ９５は、ディジタルデータを記録することができないとき、例えば表示部に警告表示をする。

【０１０４】また、ステップＳ４１において、システムコントローラ９５は、暗号解読回路８２で暗号を解読することができないと判断したとき、ステップＳ４６において、記録処理回路８７に直接出力する。記録処理回路８７は、記録に必要な処理を施し、記録手段に出力し、記録手段は、記憶部８８を構成する記録媒体に暗号圧縮されたディジタルデータを記録する。

【０１０５】次に、上記ステップＳ４３やステップＳ４４の処理で記憶部８８に記憶された暗号化され圧縮されたディジタルデータを再生するとき、記憶部８８に記憶されているディジタルデータは、再生手段により読み出された後、再生処理回路１６で再生処理が施され、再生系の暗号解読回路９０に出力される。そして、暗号解読回路９０は、暗号化回路８６で暗号化されたディジタルデータを解読し、伸長回路９１に出力し、伸長回路９１は、圧縮されたディジタルデータを伸長し、Ｄ／Ａコンバータ９２若しくはディジタル出力端子９４に出力する。そして、Ｄ／Ａコンバータ９２は、ディジタル信号をアナログ信号に変換し、アナログ出力端子９３を介して例えばスピーカに出力する。

【０１０６】以上のようなシステムでは、暗号化されたディジタルデータを解読することができないサーバ装置３ではＳＣＭＳ情報を更新せず、再生可能な記録再生装置８０にダウンロードされたときに、ＳＣＭＳ情報を更新するようにしている。したがって、このシステムでは、ネットワーク５を介してディジタルデータの送受信を行ったときにも、従来からある無断複写防止情報の管理を行うことができる。

【０１０７】なお、本発明は、上述した記録再生装置２で行う処理と記録再生装置８０で行う処理を組み合わせてもよい。すなわち、サーバ装置３を介して無断複製防止情報を含んだディジタルデータを送信先に送信するとき、送信元の記録再生装置は、送信先の装置個別鍵を取得しこれを用いてディジタルデータを暗号化してサーバ装置を介して送信先の記録再生装置に送信するようにすればよい。そして、サーバ装置は、再生機能を有していないことから無断複写防止情報を更新せず、送信先の記録再生装置は、受信したディジタルデータの暗号を解読することができるとき無断複製防止情報を更新するようにすればよい。

【０１０８】

【発明の効果】本発明によれば、記録媒体に記録された暗号化されたデータをサーバ装置に送信するとき、送信先の装置の認証を取り、認証が取れたとき、記録媒体に記録された暗号化されたデータの暗号を解読し、送信先の装置から取得した固有鍵データを用いてデータを再暗号化して出力手段から送信することから、サーバ装置に一時的にデータが記録され、このデータが権限無き第三者の端末装置にダウンロードされても、再生されることを阻止することで、著作権の保護を図ることができる。

【０１０９】また、本発明によれば、サーバ装置からダウンロードしたデータに無断複製防止情報が含まれているとき、再生可能な装置に記録されるときに限って、抽出更新手段で無断複製防止情報を抽出し更新するようにすることで、従来からある無断複写防止情報の管理を行うことができる。

【図面の簡単な説明】

【図１】本発明が適用されたデータ送受信システムを説明する図である。

【図２】上記システムに用いる記録再生装置のブロック図である。

【図３】ディジタルデータを暗号化する暗号化回路のブロック図である。

【図４】暗号解読回路のブロック図である。

【図５】記録再生装置の認証処理を説明するフローチャートである。

【図６】専用装置である記録再生装置のブロック図である。

【図７】ディジタルデータを他の装置に送信する際の手順を説明するフローチャートである。

【図８】専用装置である記録再生装置のブロック図である。

【図９】ディジタルデータを他の装置に送信する際の手順を説明するフローチャートである。

【図１０】専用装置である記録再生装置のブロック図である。

【図１１】ディジタルデータを他の装置に送信する際の手順を説明するフローチャートである。

【図１２】ネットワークを介して送信された無断複写防止情報を含むディジタルデータをダウンロードしたとき、この無断複製防止情報の更新を行う記録再生装置のブロック図である。

【図１３】図１２に示す記録再生装置の動作を説明するためのフローチャートである。

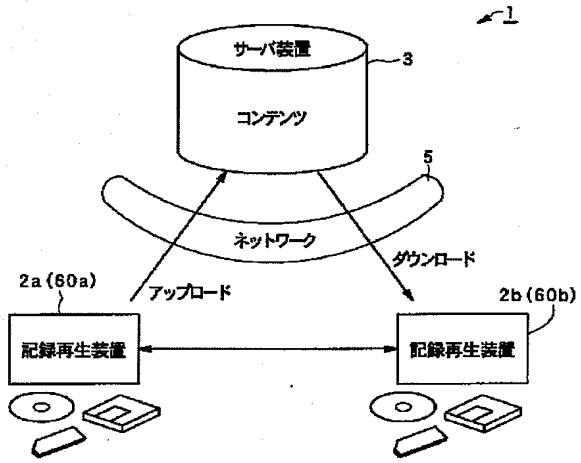
【符号の説明】

１　データ送受信システム、２（２ａ，２ｂ）　記録再生装置、３　サーバ装置、５　ネットワーク、１１　入

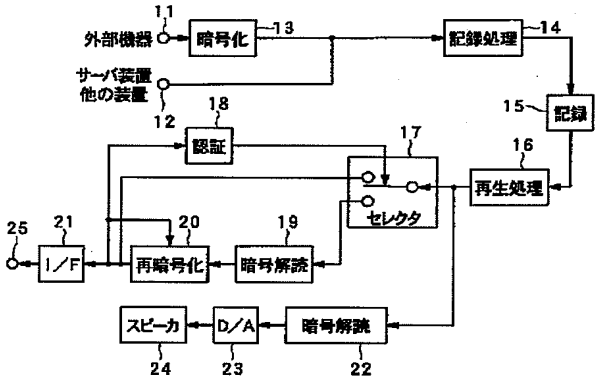
力端子、１２　入力端子、１３　暗号化回路、１４　記録処理回路、１５　記憶部、１６　再生処理回路、１７　セレクタ、１８認証回路、１９　暗号解読回路、２０　再暗号化回路、２１　通信Ｉ／Ｆ、２２　暗号解読回路、２３　Ｄ／Ａコンバータ、２４　スピーカ、２５　出力端子、３１　乱数発生回路、３２　関数回路、３３　コンテンツ鍵用メモリ、３４共通鍵用メモリ、３５　装置個別鍵用メモリ、３６　装置共通鍵生成回路、３７　コンテンツ暗号化回路、２８　コンテンツ鍵暗号化回路、４１　関数回路、４２　装置個別鍵用メモリ、４３＊10

＊　装置共通鍵生成回路、４４　暗号化鍵解読回路、４５　コンテンツ解読回路、４６　装置共通鍵用メモリ、４７　セレクタ、８０　記録再生装置（８０ａ，８０ｂ）、８１　入力端子、８２　暗号解読回路、８３　伸長回路、８４　抽出検出回路、８５　圧縮回路、８６　暗号化回路、８７　記録処理回路、８８　記憶部、８９　再生処理回路、９０　暗号解読回路、９１　伸長回路、９２　Ｄ／Ａコンバータ、９３　アナログ出力端子、９４　ディジタル出力端子、９５　システムコントローラ

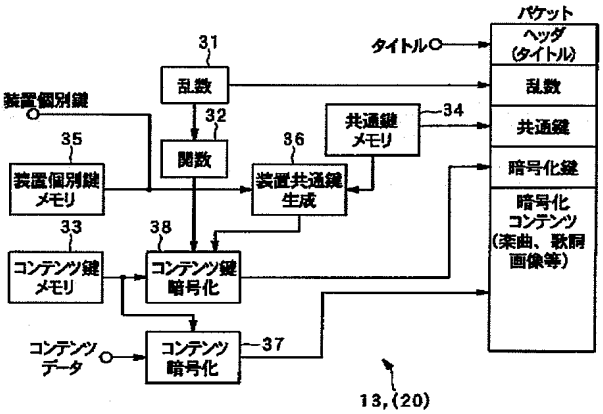
【図１】



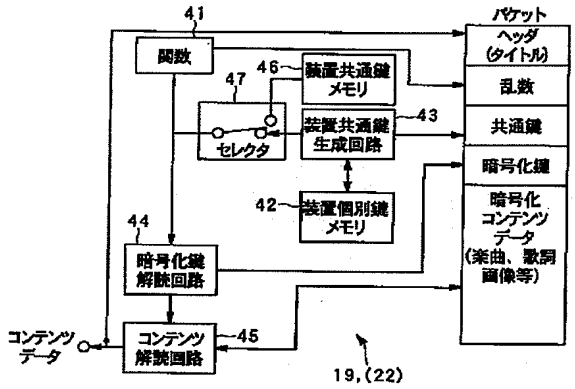
【図２】



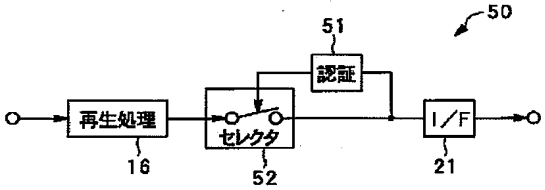
【図３】



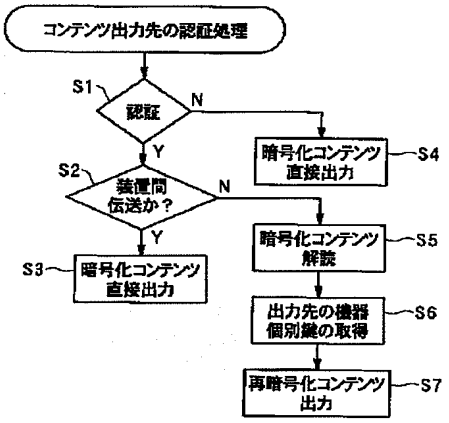
【図４】



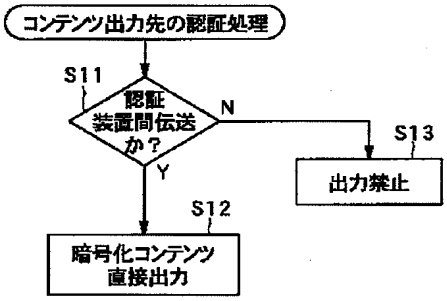
【図６】



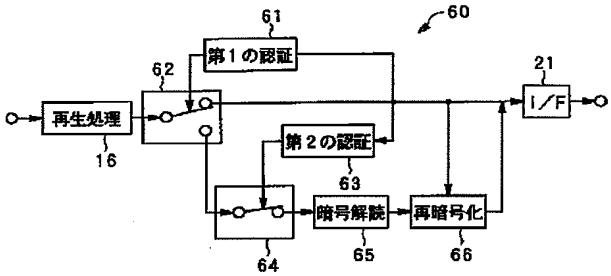
【図５】



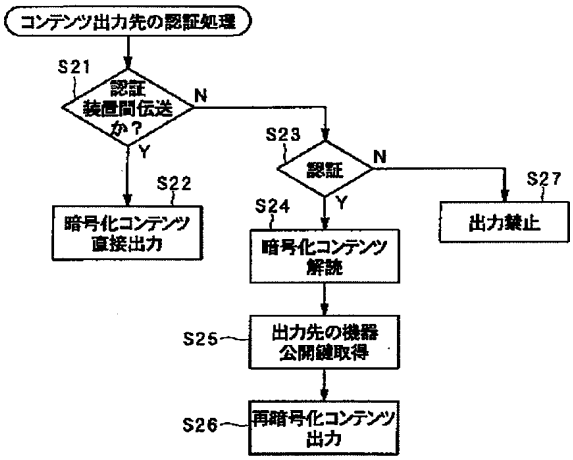
【図７】



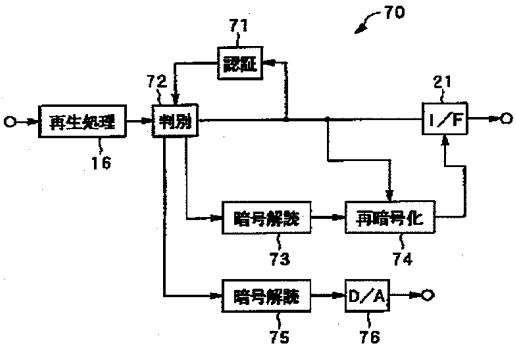
【図８】



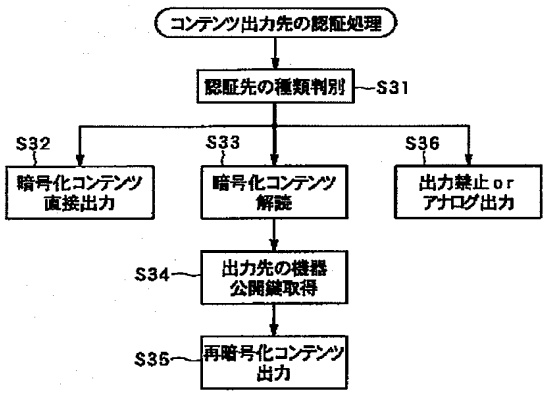
【図９】



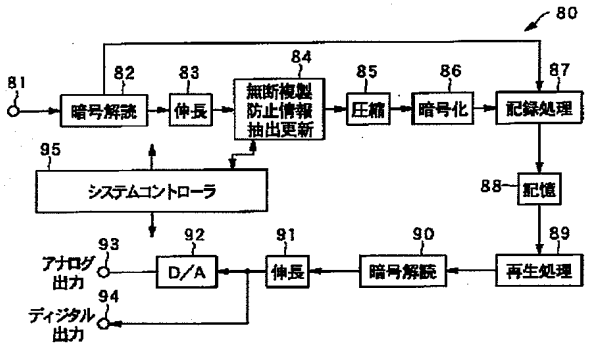
【図１０】



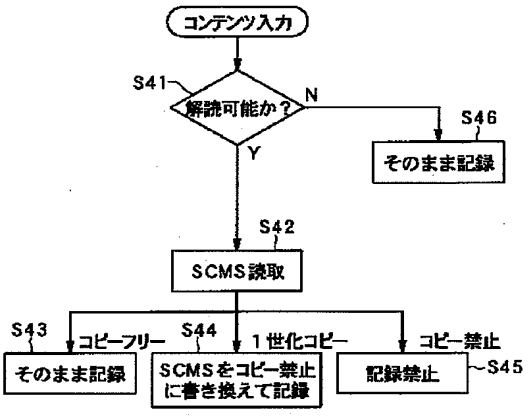
【図１１】



【図１２】



【図１３】



フロントページの続き

(72)発明者　古川　俊介
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B017 AA06 BA07 CA15
5J104 AA07 AA13 AA16 EA04 EA26
KA02 NA02 PA07 PA14

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-261748

(43)Date of publication of application : 13.09.2002

(51)Int.Cl. H04L 9/08
G06F 12/14
H04L 9/32

(21)Application number : 2001-163126

(22)Date of filing : 30.05.2001

(71)Applicant : SONY CORP

(72)Inventor : SAKO YOICHIRO
INOGUCHI TATSUYA
FURUKAWA SHUNSUKE

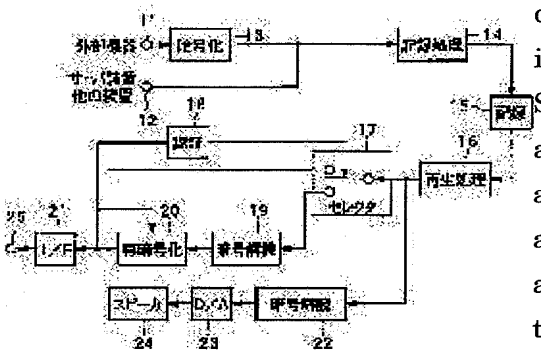
(30)Priority

Priority number : 2000403467 Priority date : 28.12.2000 Priority country : JP

(54) DATA TRANSMITTER, METHOD THEREFOR, DATA RECORDER AND METHOD THEREOF

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent copying of data without permission, even in transferring digital contents through a server device interposed inside a network.



SOLUTION: The data transmitter comprises an authenticator circuit 18 for authenticating an addressed device for receiving transmitted data, a decoder circuit 19 for decoding encrypted data and a re-encrypting circuit 20 for re- encrypting the decoded data by the deciphering circuit 19. In a recording reproducer 2, the decoder circuit 19 decodes encrypted data read from a recording medium and acquires key data unique to the addressed device, when the authenticator circuit 18 authenticates this devices, the re-encrypting circuit 20 re-encrypts the data, using the acquired unit key data, and transmits the data from a communication I/F 21. Thus the data are recorded temporarily in the server device to avoid reproducing the data, even if the data are downloaded on the terminal of an unauthorized third person.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against

examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] A regeneration means to regenerate by reading the enciphered data which were recorded on the record medium, An authentication means to take authentication of the equipment of the transmission place of the above-mentioned data, and a decryption means to decode the enciphered data to which regeneration was given with the above-mentioned regeneration means, When it has a re-encryption means to re-encipher the data decoded with the above-mentioned decryption means, and an output means to output the data enciphered by the above-mentioned re-encryption means and authentication of the equipment of the transmission place of the above-mentioned data is able to be taken with the above-mentioned authentication means, While decoding the enciphered data with which it read from the above-mentioned record medium, and regeneration was given with the above-mentioned decryption means, the proper key data of the equipment of the above-mentioned transmission place are acquired. The data source which re-enciphers the above-mentioned data with the above-mentioned re-encryption means using this acquired proper key data, and is transmitted from the above-mentioned output means.

[Claim 2] It is the data source [enable it / to output the enciphered data with which the above-mentioned means for switching read from the above-mentioned record medium when the means for switching it enables it to output from the above-mentioned output means as it is is established in the data enciphered by the above-mentioned encryption means and authentication of the equipment of the transmission place of the above-mentioned data does not take, or when authentication is not able to take, and regeneration was given to the preceding paragraph of the above-mentioned decryption means from the above-mentioned output means as it is] according to claim 1.

[Claim 3] Some data by which encryption was carried out [above-mentioned] are the data source according to claim 1 with which encryption processing is not performed.

[Claim 4] When transmitting the step which regenerates by reading the enciphered data which were recorded on the record medium, and the enciphered data which were recorded on the above-mentioned record medium, When authentication of the equipment of the step which takes authentication of the equipment of a transmission place, and the transmission place of the above-mentioned data is able to be taken, When

authentication of the equipment of the step which acquires the proper key data of the equipment of this transmission place from the equipment of the above-mentioned transmission place, and the transmission place of the above-mentioned data is able to be taken, The data transmitting and receiving method which has the step which decodes the enciphered data with which the above-mentioned regeneration was given, the step which re-enciphers the data by which decode was carried out [above-mentioned] using the proper key data of the above-mentioned transmission place, and the step which outputs the data re-enciphered [above-mentioned].

[Claim 5] The data transmitting approach according to claim 4 which outputs the enciphered data with which it read from the above-mentioned record medium, and regeneration was given when not taking authentication of the equipment of the transmission place of the above-mentioned data, or when authentication was not able to be taken as it is.

[Claim 6] Some data by which encryption was carried out [above-mentioned] are the data transmitting approaches according to claim 4 that encryption processing is not performed.

[Claim 7] The data source output the data by which encryption was carried out [above-mentioned] as it is from the above-mentioned output means when it has a regeneration means regenerate by reading the enciphered data which were recorded on the record medium, an authentication means take authentication of the equipment of the transmission place of the above-mentioned data, and an output means output the above-mentioned data and authentication of the equipment of the transmission place of the above-mentioned data is able to take by the above-mentioned authentication means.

[Claim 8] The data source according to claim 7 which forbids the output of the data from the above-mentioned output means when not taking authentication of the equipment of the transmission place of the above-mentioned data, or when authentication is not able to be taken.

[Claim 9] Furthermore, further authentication means to take authentication of other equipments used as the transmission place of the above-mentioned data, A decryption means to decode the enciphered data which it regenerated with the above-mentioned regeneration means, In the time when authentication was not able to be taken when it had a re-encryption means to re-encipher the data decoded with the above-mentioned decryption means and the above-mentioned authentication means did not take authentication of the equipment of the transmission place of the above-mentioned data When authentication of the equipment of a transmission place is able to be taken with the further authentication means, the enciphered data with which it read from the

above-mentioned record medium, and regeneration was given are decoded with the above-mentioned decryption means. the account of a top -- The data source according to claim 7 which acquires the proper key data of the equipment of the above-mentioned transmission place, re-enciphers the above-mentioned data with the above-mentioned re-encryption means using this acquired proper key data, and is outputted from the above-mentioned output means.

[Claim 10] The data transmitting approach which it has in the step which outputs as it is in the step which regenerates by reading the enciphered data which were recorded on the record medium, the step which take authentication of the equipment of a transmission place when transmitting the enciphered data which were recorded on the above-mentioned record medium, and the data by which encryption was carried out [above-mentioned] when authentication of the equipment of the transmission place of the above-mentioned data is able to take with an authentication means.

[Claim 11] The data transmitting approach according to claim 10 of forbidding the output of the above-mentioned data when not taking authentication of the equipment of the transmission place of the above-mentioned data, or when authentication is not able to be taken.

[Claim 12] In the time when authentication was not able to be taken when not taking authentication of the equipment of the transmission place of the above-mentioned data When authentication of the equipment of a transmission place is able to be taken with the further authentication means, the enciphered data with which it read from the above-mentioned record medium, and regeneration was given are decrypted. The data transmitting approach according to claim 10 which acquires the proper key data of the equipment of the above-mentioned transmission place, re-enciphers and outputs the above-mentioned data using this acquired proper key data.

[Claim 13] A regeneration means to regenerate by reading the enciphered data which were recorded on the record medium, An authentication means to take authentication of the transmission place of the above-mentioned data, and a distinction means to distinguish the class of equipment of the above-mentioned transmission place attested with the above-mentioned authentication means, A decryption means to decode the enciphered data which it regenerated with the above-mentioned regeneration means, A re-encryption means to re-encipher the data decoded with the above-mentioned decryption means by the proper key data of the equipment acquired from the equipment of the transmission place which was able to take authentication, The 1st output means which outputs the enciphered data which it regenerated with the above-mentioned regeneration means as it is, It has the 2nd output means which outputs the data

re-enciphered with the above-mentioned re-encryption means. The above-mentioned distinction means When it judges that the equipment of a transmission place is the 1st equipment, it is made to output the enciphered data which it regenerated with the above-mentioned regeneration means from the output means of the above 1st to the 1st equipment of the above as it is. When it judges that the equipment of a transmission place is the 2nd equipment, the enciphered data which it regenerated with the above-mentioned regeneration means are decoded with the above-mentioned decryption means. The data source which re-enciphers with the above-mentioned re-encryption means using the proper key data acquired from the 2nd equipment of the above, and is outputted to the 2nd equipment of the above from the output means of the above 2nd.

[Claim 14] It is the data source according to claim 13 whose 1st equipment of the above is an exclusive device and whose 2nd equipment of the above is a general-purpose device.

[Claim 15] It is the data source according to claim 13 from which, as for the 1st equipment of the above, the decryption means consists of hardware at least and which, as for the 2nd equipment of the above, the decryption means consists of with software at least.

[Claim 16] The step which regenerates by reading the enciphered data which were recorded on the record medium, The step which takes authentication of the equipment of the transmission place of the above-mentioned data, the step which distinguishes the class of equipment of the attested above-mentioned transmission place, and when a distinction result is the 1st equipment, The step which outputs the enciphered data which it regenerated to the 1st equipment as it is, and when a distinction result is the 2nd equipment, The data transmitting approach of having the step which decrypts the enciphered data which it regenerated, re-enciphers by the proper key data of the 2nd equipment of the above, and is outputted to the 2nd equipment of the above.

[Claim 17] It is the data transmitting approach according to claim 16 that the 1st equipment of the above is an exclusive device, and the 2nd equipment of the above is a general-purpose device.

[Claim 18] It is the data transmitting approach according to claim 16 that, as for the 1st equipment of the above, the decryption means consists of hardware at least, and the decryption means is constituted by software at least, as for the 2nd equipment of the above.

[Claim 19] A renewal means of an extract to extract and update unapproved duplicate prevention information from the inputted data, When record processing can be performed to the data by which the above-mentioned unapproved duplicate prevention information was updated with the above-mentioned renewal means of an extract, it can

have a record processing means to record on a record medium and the inputted above-mentioned data can be regenerated, The above-mentioned renewal means of an extract is a data recorder which controls the above-mentioned record processing means based on the above-mentioned unapproved copy prevention information while updating the above-mentioned unapproved copy prevention information.

[Claim 20] The above-mentioned unapproved copy prevention information is SCMS (Serial Copy Management System) information. The above-mentioned renewal means of an extract When the above-mentioned record processing means is controlled to record the data by which the input was carried out [above-mentioned] on the above-mentioned record medium as it is when the above-mentioned SCMS information is copy freedom and the above-mentioned SCMS information is the information which can be one-generation copied, When the above-mentioned record processing means is controlled to perform predetermined record processing to the data by which the input was carried out [above-mentioned], and to record on the above-mentioned record medium while rewriting this SCMS information to the ban on a copy, and the above-mentioned SCMS information is copy prohibition information, The data recorder according to claim 19 which forbids record to the above-mentioned record medium of the above-mentioned record processing means.

[Claim 21] The data-logging approach of having the step which extracts and updates unapproved duplicate prevention information from the inputted data, the step which performs record processing to the data with which unapproved duplicate prevention information was updated, and record to a record medium, and the step carry out record processing based on the above-mentioned unapproved copy prevention information when possible in the regeneration of data by which the input was carried out [above-mentioned].

[Claim 22] When the above-mentioned unapproved copy prevention information is SCMS (Serial Copy Management System) information and the above-mentioned SCMS information is copy freedom, When the data by which the input was carried out [above-mentioned] are recorded on the above-mentioned record medium as it is and the above-mentioned SCMS information is the information which can be one-generation copied, The data-logging approach according to claim 21 of performing predetermined record processing to the data by which the input was carried out [above-mentioned], recording on the above-mentioned record medium while rewriting this SCMS information to the ban on a copy, and forbidding record to the above-mentioned record medium when the above-mentioned SCMS information is copy prohibition information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a data recorder and an approach at the data source which prevents the unapproved copy of data, such as digital contents, and an approach list.

[0002]

[Description of the Prior Art] Copying digital contents, such as audio data, to a recordable magneto-optic disk from the optical disk only for playbacks conventionally with a digital signal is performed. In case it connects with the regenerative apparatus of an optical disk by the exclusive cable and the record regenerative apparatus of a magneto-optic disk copies digital contents, it updates the unapproved copy prevention information copied once to these digital contents as it is possible to the ban on record, and is made to perform copyright management. Therefore, the digital contents copied from the optical disk currently recorded on the magneto-optic disk can be further copied no longer to a magneto-optic disk.

[0003] Moreover, the exchange of digital contents is performed among terminal units, such as a personal computer, through networks, such as the Internet and LAN (local area network). In this case, the terminal unit of a transmitting side uploads digital contents to server equipment with the address of the terminal unit of a receiving side, and the terminal unit of a receiving side downloads the digital contents addressed to itself memorized by server equipment. In the exchange of the digital contents between which such a network was made to be placed, the count of a copy of digital contents is not managed at all in many cases.

[0004]

[Problem(s) to be Solved by the Invention] Since the system which make the network mentioned above intervene and exchanges digital contents uses a general purpose computer for a magneto-optic disk recordable from the optical disk only for playbacks not using the record regenerative apparatus of the magneto-optic disk of dedication like the system which copies digital contents, it is [system] difficult in being made updating unapproved copy prevention information, when unapproved copy prevention information added and copies to the digital contents to copy, and carrying out copyright management.

[0005] Without using a concreteness record medium, also in case the purpose of this invention makes the server equipment in a network intervene and exchanges digital

contents indirectly directly by the cable or wireless between equipment, it is to provide with a data recorder and an approach the data source and the approach list which can perform copyright management of preventing the unapproved copy of data.

[0006]

[Means for Solving the Problem] A regeneration means to regenerate by reading the enciphered data which were recorded on the record medium that the data source concerning this invention should solve the technical problem mentioned above, An authentication means to take authentication of the equipment of the transmission place of data, and a decryption means to decode the enciphered data to which regeneration was given with the regeneration means, It has a re-encryption means to re-encipher the data decoded with the decryption means, and an output means to output the data enciphered by the re-encryption means. And when authentication of the equipment of the transmission place of data is able to be taken with an authentication means, while decoding the enciphered data with which it read from the record medium and regeneration was given with a decryption means, the proper key data of the equipment of a transmission place are acquired, data are re-enciphered with a re-encryption means using this acquired proper key data, and it transmits from an output means.

[0007] Moreover, when transmitting the step which regenerates by reading the enciphered data which were recorded on the record medium that the transmitting approach of the data concerning this invention should solve the technical problem mentioned above, and the enciphered data which were recorded on the record medium, When authentication of the equipment of the step which takes authentication of the equipment of a transmission place, and the transmission place of data is able to be taken, When authentication of the equipment of the step which acquires the proper key data of the equipment of this transmission place from the equipment of a transmission place, and the transmission place of data is able to be taken, It has the step which decodes the enciphered data with which regeneration was given, the step which re-enciphers the decoded data using the proper key data of a transmission place, and the step which outputs the re-enciphered data.

[0008] Furthermore, the data source concerning this invention is equipped with a regeneration means to regenerate by reading the enciphered data which were recorded on the record medium that the technical problem mentioned above should be solved, an authentication means to take authentication of the equipment of the transmission place of data, and an output means to output data. And when authentication of the equipment of the transmission place of data is able to be taken with an authentication means, the enciphered data are outputted as it is from an output means.

[0009] Furthermore, the transmitting approach of the data concerning this invention again When transmitting the step which regenerates by reading the enciphered data which were recorded on the record medium that the technical problem mentioned above should be solved, and the enciphered data which were recorded on the record medium, When authentication of the equipment of the step which takes authentication of the equipment of a transmission place, and the transmission place of data is able to take with an authentication means, it has the step which outputs the enciphered data as it is.
[0010] Furthermore, a regeneration means to regenerate by reading the enciphered data which were recorded on the record medium that the data source concerning this invention should solve the technical problem mentioned above again, An authentication means to take authentication of the transmission place of data, and a distinction means to distinguish the class of equipment of the transmission place attested with the authentication means, A decryption means to decode the enciphered data which it regenerated with the regeneration means, A re-encryption means to re-encipher the data decoded with the decryption means by the proper key data of the equipment acquired from the equipment of the transmission place which was able to take authentication, It has the 1st output means which outputs the enciphered data which it regenerated with the regeneration means as it is, and the 2nd output means which outputs the data re-enciphered with the re-encryption means. And when the equipment of a transmission place judges a distinction means to be the 1st equipment, When it judges that it is made to output the enciphered data which it regenerated with the regeneration means from the 1st output means to the 1st equipment as it is, and the equipment of a transmission place is the 2nd equipment, The enciphered data which it regenerated with the regeneration means are decoded with a decryption means, and it re-enciphers with a re-encryption means using the proper key data acquired from the 2nd equipment, and outputs to the 2nd equipment from the 2nd output means.
[0011] Furthermore, the transmitting approach of the data concerning this invention again The step which regenerates by reading the enciphered data which were recorded on the record medium that the technical problem mentioned above should be solved, The step which takes authentication of the equipment of the transmission place of data, the step which distinguishes the class of equipment of the attested transmission place, and when a distinction result is the 1st equipment, It has the step which outputs the enciphered data which it regenerated to the 1st equipment as it is, and the step which decrypts the enciphered data which it regenerated, re-enciphers by the proper key data of the 2nd equipment, and is outputted to the 2nd equipment when a distinction result is the 2nd equipment.

[0012] Furthermore, it has a renewal means of an extract extract and update unapproved duplicate prevention information from the inputted data that the data recorder concerning this invention should solve the technical problem mentioned above, and a record processing means perform record processing to the data by which unapproved duplicate prevention information was updated with the renewal means of an extract, and record on a record medium. And when the inputted data can be regenerated, the renewal means of an extract controls a record processing means based on unapproved copy prevention information while updating unapproved copy prevention information.

[0013] Furthermore, it has the step which extracts and updates unapproved duplicate prevention information from the inputted data that the data-logging approach concerning this invention should solve the technical problem which mentioned above again, the step which perform record processing to the data with which unapproved duplicate prevention information was updated, and record to a record medium, and the step carry out record processing based on unapproved copy prevention information when possible in regeneration of the inputted data.

[0014]

[Embodiment of the Invention] Hereafter, the data transceiver system by which this invention was applied is explained with reference to a drawing.

[0015] As shown in drawing 1 , this data transceiver system 1 is equipped with the server equipment 3 in the network 5 where record regenerative-apparatus 2a which can perform record playback of digital data, such as audio data, 2b, and record regenerative-apparatus 2a and 2b are connected through a telecommunication circuit.

[0016] Server equipment 3 transmits the audio data memorized in the storage section to record regenerative-apparatus 2b, when digital data, such as audio data uploaded from one record regenerative-apparatus 2a, are temporarily memorized in the storage sections, such as a hard disk, and the download demand from record regenerative-apparatus 2b of another side is received.

[0017] Moreover, data can be directly transmitted [record regenerative-apparatus 2a and record regenerative-apparatus 2b] by connecting an exclusive cable between equipment using the interface based on IEEE(The Institute of Electronics Engineer, Inc.) 1394 specification etc. and received through server equipment 3.

[0018] Here, record regenerative-apparatus 2a and 2b are explained with reference to drawing 2 . In addition, since record regenerative-apparatus 2a and record regenerative-apparatus 2b have the same configuration, they are also only called record regenerative apparatus 2 below.

[0019] This record regenerative apparatus 2 has the input terminal 11 into which digital data, such as audio data outputted from the external instrument, are inputted, and the input terminal 12 into which the digital data enciphered from other record regenerative apparatus 2 through the network 5 is inputted from server equipment 3. Moreover, a record regenerative apparatus 2 has the storage section 15 which consists of the hard disk with which the digital data enciphered as the encryption circuit 13 which enciphers the digital data inputted from the input terminal 11, and the record processing circuit 14 which performs record processing of the enciphered digital data is recorded, a recordable optical disk, a magneto-optic disk, semiconductor memory, an IC card, etc., and the regeneration circuit 16 which regenerate the digital data read from playback means, such as the magnetic head and an optical pickup.

[0020] moreover, this record regenerative apparatus 2 as a transmitting system for transmitting digital data to server equipment 3 or other record regenerative apparatus 2 The digital data enciphered as the path which outputs the enciphered digital data as it is The selector 17 which enciphers and switches the path to output, [re-] The authentication circuit 18 which takes authentication of the transmission place of digital data and controls a selector 17 based on an authentication result, The decryption circuit 19 which decodes the enciphered digital data, and the re-encryption circuit 20 which re-enciphers the digital data decrypted in the decryption circuit 19, The communication link interface for performing server equipment 3, other record regenerative apparatus 2, and data communication (it is also only hereafter called communication link I/F.) It has 21.

[0021] Furthermore, the record regenerative apparatus 2 is equipped with the decryption circuit 22 where the output from the regeneration circuit 16 is inputted, D/A converter 23 which changes the decrypted digital data into an analog signal from a digital signal, and the loudspeaker 24 which transduces electroacoustically and outputs the data changed into the analog signal as a reversion system of the digital data recorded on the storage section 15.

[0022] The encryption circuit 13 enciphers the digital data inputted from the input terminal 11 using the equipment individual key memorized by memory. The random-number-generation circuit 31 where this encryption circuit 13 generates a random number concretely as shown in drawing 3 , The function circuit 32 which generates the function based on a random number, and the memory 33 for contents keys which memorizes the contents key which enciphers contents, The memory 34 for common keys which memorizes the common key used in order to encipher a contents key, The memory 35 for equipment individual keys which records the equipment

individual key of the proper of the record regenerative apparatus 2, The equipment common key generation circuit 36 which generates the equipment common key common to all the record regenerative apparatus 2 with a common key and an equipment individual key, It has the contents key encryption circuit 38 which enciphers a contents key with the contents encryption circuit 37 which enciphers contents with a contents key, and an equipment common key and the function with which the random number was given.

[0023] If digital data is inputted into the encryption circuit 13, from the memory 33 for contents keys, a predetermined contents key will be read, it will encipher except for headers, such as a title, using this contents key, and the contents encryption circuit 37 will output encryption contents. With this, the random-number-generation circuit 31 generates a random number, and outputs this random number to the function circuit 32, and the function circuit 32 generates a function based on a random number. Moreover, the equipment common key generation circuit 36 reads a common key from the memory 34 for common keys, reads an equipment proper key from the memory 35 for equipment proper keys, and generates an equipment common key based on a common key and an equipment proper key. The contents key used for enciphering contents is outputted also to the contents key encryption circuit 38 from the contents key encryption circuit 38, and this contents key encryption circuit 38 is with the function which the random number was given and was generated in the function circuit 32, and the equipment common key generated in the equipment common key generation circuit 36, and generates an encryption key.

[0024] And the encryption circuit 13 generates the following packets. That is, the packet generated by this encryption circuit 13 consists of the header which consists of a title of the contents which are not enciphered etc., the random number generated in the random-number-generation circuit 31, a common key outputted from the memory 34 for common keys, an encryption key outputted from the contents key encryption circuit 38, and encryption contents outputted from the contents encryption circuit 37.

[0025] And since the encryption circuit 13 which generated the above packets processes for recording on the storage section 15, it outputs to the record processing circuit 14 per packet. The digital data enciphered in the encryption circuit 13 and the digital data enciphered from the server equipment 3 inputted from the input terminal 12 or other record regenerative apparatus 2 are inputted into the record processing circuit 14. This record processing circuit 14 performs and makes binary error correction coding processing and modulation processing to the data these-inputted, for example. And the data with which record processing was performed are recorded on the record medium

which constitutes the storage section 15 with record means, such as the magnetic head and an optical pickup. In addition, the storage section 15 may be built in the body of equipment, and may be removable to the body of equipment.

[0026] Moreover, the data memorized by the storage section 15 are also read from a record medium by playback means, such as the magnetic head and an optical pickup. And the read data are outputted to the regeneration circuit 16. The regeneration circuit 16 makes an output binary from a playback means, performs recovery processing and error correction processing, and outputs them to communication link I/F21 of a transmitting system, or the decryption circuit 22 of a reversion system.

[0027] The authentication circuit 18 takes authentication of the record regenerative apparatus 2 of a transmission place, and carries out change-over control of the selector 17 based on the authentication result. Moreover, even if the authentication circuit 18 is the time when authentication of the record regenerative apparatus 2 of a transmission place was able to be taken, change-over control of a selector 17 is performed by whether digital data is directly transmitted to the record regenerative apparatus 2 by whether it transmits to other record regenerative apparatus 2 through server equipment 3, and the exclusive cable. A selector 17 is switched so that it can output while the digital data had been enciphered when authentication is not able to be taken in the authentication circuit 18, and when it can take authentication and digital data is directly outputted to other record regenerative apparatus 2, and when authentication can be taken and it outputs to other record regenerative apparatus 2 through server equipment 3, it is switched so that re-encryption can be carried out.

[0028] In case the decryption circuit 19 which constitutes a transmitting system transmits digital data, it decodes the digital data enciphered in the encryption circuit 13 mentioned above in order to re-encipher with the equipment individual key of the record regenerative apparatus 2 of the transmission place acquired from the transmission place, and outputs it to the re-encryption circuit 20. The function circuit 41 which generates a function concretely based on the random number in a packet as this decryption circuit 29 is shown in drawing 4 , The memory 42 for equipment individual keys the same key as the memory 35 for equipment individual keys of the above-mentioned encryption circuit 13 is remembered to be, The equipment common key generation circuit 43 which generates an equipment common key with the common key in a packet, and the equipment individual key read from the memory 42 for equipment individual keys, The encryption key decode circuit 44 which decodes the encryption key in a packet with the function generated in the function circuit 41, and the equipment common key generated in the equipment common key generation circuit

43, It has the contents decode circuit 45 which decodes the encryption contents in a packet based on the contents key decoded in the encryption key decode circuit 44.

[0029] If the digital data enciphered by the decryption circuit 19 is inputted, the function circuit 41 generates a function based on the random number in a packet, and from the common key in a packet, and the memory 42 for equipment individual keys, the equipment common key generation circuit 43 will read an equipment individual key, and will generate an equipment common key, and it will output it to the encryption key decode circuit 44. The encryption key decode circuit 44 decodes the encryption key read from the inside of a packet with the function generated in the function circuit 41, and the equipment common key, generates a contents key, and outputs it to the contents decode circuit 45. From the inside of a packet, the contents decode circuit 45 reads encryption contents, and decodes this using a contents key. In addition, since the header in a packet is not enciphered, the decryption circuit 19 is read from the inside of a packet as it is. And the decryption circuit 19 outputs the digital data after decryption to the re-encryption circuit 20.

[0030] When authentication can be taken and is outputted to other record regenerative apparatus 2 through server equipment 3, the re-encryption circuit 20 acquires an equipment individual key from the record regenerative apparatus 2 of a transmission place, and re-enciphers the digital data outputted using this equipment individual key. Since this re-encryption circuit 20 has the almost same configuration as the encryption circuit 13 shown in above-mentioned drawing 3 , although omitted for details, the equipment individual key of the transmission place read from the memory 35 for equipment individual keys of other record regenerative apparatus 2 of the transmission place of digital data is inputted into the equipment common key generation circuit 36 from the memory 35 for equipment individual keys. And as mentioned above, the re-encryption circuit 20 generates the packet which consists of the header which is not enciphered, the random number generated in the random-number-generation circuit 31, the common key outputted from the memory 34 for common keys, an encryption key outputted from the contents key encryption circuit 38, and encryption contents outputted from the contents encryption circuit 37, and outputs it to communication link I/F21.

[0031] When performing transmission protocols, such as TCP/IP (transmission control protocol/internet protocol), transmitting the digital data re-enciphered by server equipment 3 through an output terminal 25, when transmitting to server equipment 3, and transmitting to other record regenerative apparatus 2 directly by the exclusive cable, communication link I/F21 performs an IEEE1394 protocol etc., and transmits to

other record regenerative apparatus 2 through an output terminal 25.

[0032] In case the decryption circuit 22 which constitutes a reversion system reproduces the enciphered digital data which is memorized by the storage section 15, it decodes the digital data enciphered in the encryption circuit 13. In addition to the configuration of the decryption circuit 19 shown in above-mentioned drawing 4 , this decryption circuit 22 is omitted further for details, but it has the selector 47 which switches the memory 46 for equipment common keys which memorizes an equipment common key, and the output from the equipment common key generation circuit 43 and the output from the memory 46 for equipment common keys.

[0033] When a selector 47 reproduces the digital data downloaded from server equipment 3, When reproducing the digital data which switched so that the equipment common key generated in the equipment common key generation circuit 43 might be outputted to the encryption key decode circuit 44, and was directly transmitted through the exclusive cable from other record regenerative apparatus 2, It switches so that the equipment common key memorized by the memory 46 for equipment common keys may be outputted to the encryption key decode circuit 44. And the decryption circuit 22 outputs the decrypted digital data to D/A converter 23. D/A converter 23 changes the decrypted digital data into an analog signal, and a loudspeaker 24 transduces the data of this analog electroacoustically and outputs it.

[0034] In the above record regenerative apparatus 2, if the actuation which saves digital data, such as audio data outputted from the external instrument, in the storage section 15 is explained, the digital data read from external storage will be inputted from an input terminal 11, and will be enciphered by the encryption circuit 13. Namely, if digital data is inputted into the encryption circuit 13, from the memory 33 for contents keys, the contents encryption circuit 37 will read a predetermined contents key, and will encipher it except for headers, such as a title, using this contents key. With this, the random-number-generation circuit 31 generates a random number, and outputs this random number to the function circuit 32, and the function circuit 32 generates a function based on a random number. Moreover, the equipment common key generation circuit 36 reads a common key from the memory 34 for common keys, reads an equipment proper key from the memory 35 for equipment individual keys, and generates an equipment common key based on a common key and an equipment proper key. The contents key used for enciphering contents is outputted also to the contents key encryption circuit 38 from the contents key encryption circuit 38, and this contents key encryption circuit 38 is with the function which the random number was given and was generated in the function circuit 32, and the equipment common key generated in the

equipment common key generation circuit 36, and generates an encryption key. And the encryption circuit 13 generates the packet which consists of the header which is not enciphered, the random number generated in the random-number-generation circuit 31, the common key outputted from the memory 34 for common keys, an encryption key outputted from the contents key encryption circuit 38, and encryption contents outputted from the contents encryption circuit 37.

[0035] And this packet is recorded on the storage section 15 by the record means, after record processing is made in the record processing circuit 14. In the record regenerative apparatus 2, although the digital data is memorized after having been enciphered by the Records Department 15, the header is not enciphered. Therefore, the record regenerative apparatus 2 can find out easily the digital data which can search easily the digital data enciphered by the storage section 15 with using a header, for example, is transmitted, and the digital data to reproduce.

[0036] Next, the authentication processing at the time of record regenerative-apparatus 2a of the transmitting origin constituted as mentioned above transmitting digital data to other record regenerative-apparatus 2bs is explained with reference to drawing 5 .

[0037] First, in step S1, if transmitting actuation of transmitting the enciphered digital data which is memorized by the user at the storage section 15 is carried out, in step S1, the authentication circuit 18 of record regenerative-apparatus 2a of a transmitting agency will attest whether it is equipment with which record regenerative-apparatus 2b of a transmission place was based on the same specification. Concretely, record regenerative-apparatus 2a attests record regenerative-apparatus 2b of a transmission place through server equipment 3 through an exclusive cable. And record regenerative-apparatus 2a of a transmitting agency progresses to step S2, when authentication of record regenerative-apparatus 2b of a transmission place is able to be taken, and when authentication is not able to be taken, it progresses to step S4.

[0038] In step S2, record regenerative-apparatus 2a of a transmission place judges whether transmission of digital data is direct transmission which used the exclusive cable, or it is indirect transmission through server equipment 3, and chooses the transmitting approach of digital data and the method of communication link I/F21 to transmit. And record regenerative-apparatus 2a of a transmitting agency progresses to step S3, when it is direct transmission which used the exclusive cable, and when it is indirect transmission through server equipment 3, it progresses to step S5.

[0039] When it is direct transmission using an exclusive cable, since record regenerative-apparatus 2b of a transmission place is regular equipment which was able to take authentication and is equipment which also has a decryption function

corresponding to its encryption, in step S3, the record regenerative-apparatus 2a of a transmitting agency outputs the enciphered digital data to record regenerative-apparatus 2b of a transmission place through an exclusive cable as it is. That is, the selector 17 of record regenerative-apparatus 2a of a transmitting agency carries out direct continuation of the regeneration circuit 16 and communication link I/F21, as shown in drawing 2 . Thereby, the enciphered digital data which is memorized by the storage section 15 is outputted to record regenerative-apparatus 2b of a transmission place from communication link I/F21 as it is, after regeneration is given in the regeneration circuit 16. Therefore, since record regenerative-apparatus 2a of a transmitting agency does not have the need of performing decryption and re-encryption processing, it can transmit digital data to a high speed at the record regenerative apparatus 2 of a transmission place.

[0040] After the digital data enciphered is inputted into record regenerative-apparatus 2b of a transmission place from an input terminal 12 and record processing is made in the record processing circuit 14, it is recorded on the storage section 15 by the record means. Here, although the digital data enciphered by the storage section 15 will be memorized in record regenerative-apparatus 2b of a transmission place, a header can search the digital data to reproduce easily from not being enciphered. And when reproducing the enciphered digital data which is recorded on the storage section 15, regeneration is given in the regeneration circuit 16 and the enciphered digital data which was read by the playback means is outputted to the decryption circuit 22 of a reversion system.

[0041] As shown in drawing 4 , the decryption circuit 22 is switched so that the equipment common key memorized in the selector 47 by the memory 46 for equipment common keys can be outputted to the encryption key decode circuit 44. And if the digital data enciphered in the encryption circuit 13 of record regenerative-apparatus 2a of a transmitting agency is inputted, the function circuit 41 will generate a function based on the random number in a packet, and the encryption key decode circuit 44 will read the equipment common key memorized by the memory 46 for equipment common keys. The encryption key decode circuit 44 decodes the encryption key read from the inside of a packet with the function generated in the function circuit 41, and the equipment common key, generates a contents key, and outputs it to the contents decode circuit 45. From the inside of a packet, the contents decode circuit 45 reads encryption contents, and decodes this using a contents key. In addition, since the header in a packet is not enciphered, the decryption circuit 22 is read from the inside of a packet as it is. And the decryption circuit 22 outputs the decrypted digital data to D/A converter 23. D/A

converter 23 changes the decrypted digital data into an analog signal, and a loudspeaker 24 transduces the data of this analog electroacoustically and outputs it.

[0042] Moreover, in step S1, record regenerative-apparatus 2a of a transmitting agency outputs the enciphered digital data to record regenerative-apparatus 2b of a transmission place through server equipment 3 in step S4 through an exclusive cable as it is, also when authentication of record regenerative-apparatus 2b of a transmission place is not able to be taken. That is, as shown in drawing 2 , record regenerative-apparatus 2a of a transmission place switches a selector 17, and carries out direct continuation of the regeneration circuit 16 and communication link I/F21. Thereby, the enciphered digital data which is memorized by the storage section 15 is outputted to record regenerative-apparatus 2b of a transmission place from communication link I/F21 as it is, after regeneration is given in the regeneration circuit 16. After the digital data enciphered is inputted into record regenerative-apparatus 2b of a transmission place from an input terminal 12 and record processing is made in the record processing circuit 14, it is recorded on the storage section 15 by the record means.

[0043] Here, record regenerative-apparatus 2b of a transmission place is equipment which was not able to take authentication, and cannot decode the enciphered digital data from not having the decryption function. Therefore, even if digital data passes into those who are not regular users, it can prevent that this digital data is reproduced.

[0044] Moreover, in step S2, when it judges that record regenerative-apparatus 2a of a transmitting agency is indirect transmission through server equipment 3, after the enciphered digital data which is recorded on the storage section 15 is read by the playback means, in step S5, regeneration is given in the regeneration circuit 16. Here, a selector 17 connects the regeneration circuit 16 and the decryption circuit 19 so that re-encryption can be carried out.

[0045] And if the digital data enciphered by the decryption circuit 19 is inputted, as shown in drawing 4 , the function circuit 41 generates a function based on the random number in a packet, and from the common key in a packet, and the memory 42 for equipment individual keys, the equipment common key generation circuit 43 will read an equipment individual key, and will generate an equipment common key, and it will output it to the encryption key decode circuit 44. The encryption key decode circuit 44 decodes the encryption key read from the inside of a packet with the function generated in the function circuit 41, and the equipment common key, generates a contents key, and outputs it to the contents decode circuit 45. From the inside of a packet, the contents decode circuit 45 reads encryption contents, and decodes this using a contents key. In addition, since the header in a packet is not enciphered, the decryption circuit 19 is read

from the inside of a packet as it is. And the decryption circuit 19 outputs the digital data after decryption to the re-encryption circuit 20.

[0046] Subsequently, in step S6, record regenerative-apparatus 2a of a transmitting agency acquires an equipment individual key from the memory 35 for equipment individual keys of record regenerative-apparatus 2b of a transmission place through server equipment 3 so that decryption may be possible in record regenerative-apparatus 2b of the transmission place which was able to take authentication.

[0047] Subsequently, in step S7, record regenerative-apparatus 2a of a transmitting agency performs re-encryption in the re-encryption circuit 20 using the equipment individual key again acquired at step S6 to the digital data decrypted in the decryption circuit 19. Namely, if digital data is inputted into the re-encryption circuit 20, from the memory 33 for contents keys, the contents encryption circuit 37 will read a predetermined contents key, and will encipher it except for headers, such as a title, using this contents key. With this, the random-number-generation circuit 31 generates a random number, and outputs this random number to the function circuit 32, and the function circuit 32 generates a function based on a random number. Moreover, the equipment common key generation circuit 36 generates an equipment common key based on the common key which read the common key from the memory 34 for common keys, and the equipment proper key acquired from record regenerative-apparatus 2b of a transmission place. The contents key used for enciphering contents is outputted also to the contents key encryption circuit 38 from the contents key encryption circuit 38, and this contents key encryption circuit 38 is with the function which the random number was given and was generated in the function circuit 32, and the equipment common key generated in the equipment common key generation circuit 36, and generates an encryption key. And the re-encryption circuit 20 generates the packet which consists of the header which is not enciphered, the random number generated in the random-number-generation circuit 31, the common key outputted from the memory 34 for common keys, an encryption key outputted from the contents key encryption circuit 38, and encryption contents outputted from the contents encryption circuit 37, and outputs it to communication link I/F21.

[0048] In this way, it is transmitted to server equipment 3 through a network 5, and the digital data with which re-encryption was carried out is saved temporarily. At this time, the terminal unit which does not have authority accesses server equipment 3, and even if it is a time of downloading the digital data which record regenerative-apparatus 2a transmitted, and saving in the storage section, this terminal unit cannot decode a code. Therefore, the digital data currently temporarily recorded on server equipment 3 can

prevent being reproduced with a user's terminal unit which authority does not have. Moreover, since the header is not enciphered also when the digital data with which many were enciphered is saved to server equipment 3, the data of server equipment 3 can be easily searched from record regenerative-apparatus 2a and 2b.

[0049] Record regenerative-apparatus 2b of a transmission place can download the digital data addressed to itself by accessing server equipment 3. The downloaded digital data which is enciphered is recorded on the storage section 15 by the record means, after being inputted from an input terminal 12 and making record processing in the record processing circuit 14. Here, although the digital data enciphered by the storage section 15 will be memorized in record regenerative-apparatus 2b of a transmission place, a header can search the digital data to reproduce easily from not being enciphered. If regeneration is given in the regeneration circuit 16 after being read by the playback means when reproducing the enciphered digital data which is recorded on the storage section 15, it will be outputted to the decryption circuit 22 of a reversion system.

[0050] Here, as shown in drawing 4 , a selector 47 is switched so that the equipment common key generated in the equipment common key generation circuit 43 may be outputted to the encryption key decode circuit 44. And if the digital data enciphered by the encryption circuit 13 is inputted, the function circuit 41 generates a function based on the random number in a packet, and from the common key in a packet, and the memory 42 for equipment individual keys, the equipment common key generation circuit 43 will read an equipment individual key, and will generate an equipment common key, and it will output it to the encryption key decode circuit 44. Here, the record regenerative apparatus 2 of a transmitting agency of the equipment individual key of the memory 42 for equipment individual keys of record regenerative-apparatus 2b is the same as that of what was acquired at step S6. The encryption key decode circuit 44 decodes the encryption key read from the inside of a packet with the function generated in the function circuit 41, and the equipment common key, generates a contents key, and outputs it to the contents decode circuit 45. From the inside of a packet, the contents decode circuit 45 reads encryption contents, and decodes this using a contents key. In addition, since the header in a packet is not enciphered, the decryption circuit 22 is read from the inside of a packet as it is. And the decryption circuit 22 outputs the decrypted digital data to D/A converter 23. D/A converter 23 changes the decrypted digital data into an analog signal, and a loudspeaker 24 transduces the data of this analog electroacoustically and outputs it.

[0051] in the above systems, even if the record regenerative apparatus which does not

have authority may download the digital data temporarily saved to server equipment 3 and it may save it in the storage section, since it is enciphered, this digital data is reproduced with the record regenerative apparatus which does not have authority -- things -- there is nothing. Therefore, copyright management can be performed in this system, without putting in unapproved copy prevention information into digital data.

[0052] In addition, although it explained above taking the case of the case where an exclusive cable is used when transmitting digital data between record regenerative-apparatus 2a and 2b, it may be made to carry out on radio.

[0053] Next, other examples which exchange digital data between record regenerative-apparatus 2a and record regenerative-apparatus 2bs which are the exclusive device of this system are explained. Record regenerative-apparatus 2a and 2b are exclusive devices which exchange data directly by the cable or wireless, and are used for this system. Therefore, it faces communicating digital data and is a safe environment. Then, record regenerative-apparatus 2a of a transmitting agency forbids the output of digital data, when the digital data enciphered when authentication of record regenerative-apparatus 2b of a transmission place is able to be taken is transmitted to record regenerative-apparatus 2b as it was and authentication is not able to be taken. Moreover, in this example, in order to raise the safety in the case of data communication, the exchange is made not to carry out digital data through server equipment 3 with equipment accessible like an above-mentioned example without authority. Hereafter, this example is explained with reference to drawing 6 and drawing 7 .

[0054] As shown in drawing 6 , this record regenerative apparatus 50 As a transmitting system for having the same configuration except for the record regenerative apparatus 2 shown in drawing 2 , and a transmitting system, and transmitting digital data to other record regenerative apparatus 2 It has the authentication circuit 51 which attests the equipment of the transmission place of data, and the selector 52 which enables the output of data in the authentication circuit 51 whenever it was able to take authentication of the equipment of a transmission place.

[0055] The authentication circuit 51 takes authentication of the equipment of a transmission place, and carries out change-over control of the selector 52 based on an authentication result. That is, it switches a selector 52 so that the regeneration circuit 16 and communication link I/F21 may be connected, noting that transmission of the enciphered digital data is possible for the authentication circuit 51, when the equipment of a transmission place is the record regenerative apparatus 50 which is an exclusive device. Moreover, the equipment to transmit is server equipment 3, or the

authentication circuit 51 is a personal computer which is a general-purpose device, and it switches a selector 52 so that the regeneration circuit 16 and communication link I/F53 may not be connected, in order to forbid the output of the enciphered digital data, when it is not the record regenerative apparatus 50.

[0056] Next, the procedure at the time of the record regenerative apparatus 50 transmitting digital data to other equipments is explained using drawing 7 . First, if transmitting actuation of transmitting the enciphered digital data which is memorized by the user in step S11 at the storage section 15 is carried out, it will judge whether the authentication circuit 51 of the record regenerative apparatus 50 of a transmitting agency has equipment of a transmission place with the record regenerative apparatus 50. That is, even if a transmission place is the record regenerative apparatus 50, when the equipment of a transmission place is general-purpose devices, such as a personal computer, directly or the authentication circuit 51 is server equipment 3 directly, it is made not to attest the equipment of a transmission place. It is because there is a possibility that the digital data which a possibility of downloading unjustly is in the equipment which does not have authority in transmitting to server equipment 3, it cannot necessarily say that it is a safe environment, but the software which decodes a code in transmitting to the personal computer which is a general-purpose device is unjustly installed in the personal computer, and was enciphered may be decoded unjustly. So, in the record regenerative apparatus 50, whenever direct continuation of the record regenerative apparatus 50 which is an exclusive device is carried out, it can be made to perform transmission of digital data.

[0057] And in step S12, when transmitting digital data to the record regenerative apparatus 50 directly, the authentication circuit 51 switches a selector 52 so that the regeneration circuit 16 and communication link I/F21 may be connected. And the record regenerative apparatus 50 transmits the digital data enciphered by the record regenerative apparatus 50 of a transmission place.

[0058] Moreover, even if a transmission place is the record regenerative apparatus 50, when the equipment of a transmission place is general-purpose devices, such as a personal computer, directly or the authentication circuit 51 is server equipment 3 directly, it turns OFF connection between the regeneration circuit 16 and communication link I/F21 in step S13. That is, the record regenerative apparatus 50 forbids the output of the enciphered digital data to the equipment of a transmission place.

[0059] When digital data can be transmitted in a completely safe environment, digital data can be safely transmitted [the above record regenerative apparatus 50] and

received by permitting the output of the enciphered digital data only within the case where it outputs to the record regenerative apparatus 50 directly. Moreover, when transmitting digital data, since it is transmitted to the record regenerative apparatus 50 of a transmission place, without carrying out re-encryption, the digital data saved after having been enciphered by the storage section 15 can save the time amount for re-encryption.

[0060] In addition, although the above example explained the case where digital data could be outputted only within the case where the equipment of a transmission place is the record regenerative apparatus 50, if the equipment of a transmission place is equipment which can output digital data in a safe environment, it will not be limited to the record regenerative apparatus 50. For example, since it is equipment which can be trusted and an exchange of data can carry out to insurance when the equipment with which the decryption circuit based on this system etc. consisted of semiconductor chips of dedication etc. is equipment of a transmission place, you may make it permit the output of digital data.

[0061] Next, the example which can be outputted when authentication is able to be taken in the personal computer which is a general-purpose device besides the record regenerative apparatus which is the exclusive device of this system about digital data is explained with reference to drawing 8 and drawing 9 .

[0062] As shown in drawing 8 , this record regenerative apparatus 60 As a transmitting system which transmits the digital data which has the same configuration as the record regenerative apparatus 2 shown in drawing 2 except for a transmitting system, and was enciphered to other equipments The 1st authentication circuit 61 which attests whether it is the record regenerative apparatus 60 whose equipment of a transmission place is the exclusive device of this system, The digital data enciphered as the path which outputs the enciphered digital data as it is The 1st selector 62 which enciphers and switches the path to output, [re-] The 2nd authentication circuit 63 which attests whether the equipment of a transmission place is general-purpose devices, such as a personal computer, The 2nd selector 64 which permits the output of the digital data enciphered when authentication of a general-purpose device was able to be taken in the 2nd authentication circuit 63, It has the decryption circuit 65 which decodes the enciphered digital data, and the re-encryption circuit 66 which re-enciphers the digital data decrypted in the decryption circuit 65.

[0063] The 1st authentication circuit 61 takes authentication of the equipment of a transmission place, and carries out change-over control of the selector 52 based on an authentication result. That is, the equipment of a transmission place is the record

regenerative apparatus 60 which is an exclusive device, and it switches the 1st selector 62 so that the regeneration circuit 16 and communication link I/F21 may be connected, noting that transmission of the enciphered digital data is possible for the 1st authentication circuit 61, when transmitting digital data to this record regenerative apparatus 60 directly. Moreover, even if it is the case where digital data is transmitted directly even if it is the record regenerative apparatus 60, when transmitting through server equipment 3, when transmitting to general-purpose devices, such as a personal computer, the 1st authentication circuit 61 cuts the regeneration circuit 16 and communication link I/F21, and it switches them so that the regeneration circuit 16 and the 2nd selector 64 may be connected.

[0064] The 2nd authentication circuit 63 is equipment with which the software for decryption of a transmission place by general-purpose devices, such as a personal computer, was installed in normal, or performs authentication of the record regenerative apparatus 60 at the time of transmitting to the record regenerative apparatus 60 or a general-purpose device through server equipment 3, or a general-purpose device, and carries out change-over control of the 2nd selector 64 based on an authentication result. Namely, the case where the 2nd authentication circuit 63 transmits the digital data with which the software for decryption was enciphered by the general-purpose device installed in normal, The case where the digital data enciphered by the record regenerative apparatus 60 through server equipment 3 is transmitted, When transmitting the digital data enciphered by the general-purpose device by which software was installed in normal through server equipment 3, the 2nd selector 64 is switched to the condition of the ON which connects the regeneration circuit 16 and the decryption circuit 65 through the 1st selector 62. Moreover, the 2nd authentication circuit 63 switches the 2nd selector 64 to the off condition of not connecting the regeneration circuit 16 and the decryption circuit 65, when authentication of the equipment of a transmission place is not able to be taken. The 2nd authentication circuit 63 is changed into the condition against [of digital data] an output.

[0065] In case the decryption circuit 65 transmits digital data, it decodes the digital data enciphered in the encryption circuit 13 mentioned above in order to re-encipher, and outputs it to the re-encryption circuit 66.

[0066] The re-encryption circuit 66 acquires a public key from the general-purpose device which was able to take authentication in the 2nd authentication circuit 63, and re-enciphers digital data using this public key. And the re-encryption circuit 66 outputs the re-enciphered digital data to communication link I/F21.

[0067] Next, the procedure at the time of the record regenerative apparatus 60

transmitting digital data to other equipments is explained using drawing 9 . If transmitting actuation of transmitting the enciphered digital data which is memorized by the user at the storage section 15 is carried out, it will judge whether the 1st authentication circuit 61 of the record regenerative apparatus 60 of a transmitting agency has equipment of a transmission place with the record regenerative apparatus 60 in step S21. That is, it judges whether the 1st authentication circuit 61 transmits digital data for whether digital data is directly transmitted to the record regenerative apparatus 60 to equipments other than record regenerative-apparatus 60.

[0068] When the equipment of a transmission place was the record regenerative apparatus 60 and authentication is able to be taken, the 1st authentication circuit 61 switches the 1st selector 62 in step S22 so that digital data can be outputted to communication link I/F21 from the regeneration circuit 16. The enciphered digital data which was read from the storage section 15 is transmitted to the record regenerative apparatus 60 of a transmission place from communication link I/F21 in the condition [being enciphered] by this. In this case, since the record regenerative apparatus 60 does not perform re-encryption, it can transmit digital data to a high speed. When reproducing this digital data, using a common key, the record regenerative apparatus 60 of a transmission place decodes a code, and is reproduced.

[0069] When the 1st authentication circuit 61 does not attest the equipment of a transmission place in step S21, in step S23, the 2nd authentication circuit 63 attests the equipment of a transmission place. That is, the 2nd authentication circuit 63 judges ********, when the equipment to which the software for decryption of the equipment connected through direct or server equipment 3 was connected [whether it is the general-purpose device installed in normal and] through server equipment 3 is the record regenerative apparatus 60.

[0070] And when authentication of the equipment of a transmission place is able to be taken in the 2nd authentication circuit 63, in step S24, the 2nd authentication circuit 63 switches the 2nd selector 64 to the condition of the ON which connects the regeneration circuit 16 and the decryption circuit 65 through the 1st selector 62. And the digital data which was read from the storage section 15 and which is enciphered is inputted into the decryption circuit 65. And the decryption circuit 65 decodes the digital data enciphered in the encryption circuit 13 mentioned above in order to re-encipher, and outputs it to the re-encryption circuit 66.

[0071] The re-encryption circuit 66 acquires the public key of the equipment of a transmission place in step S25. In step S26, the re-encryption circuit 66 enciphers again the digital data decrypted in the decryption circuit 62. And communication link I/F20

transmits this re-enciphered digital data to the equipment of a transmission place. That is, when the equipment of a transmission place is a general-purpose device or it transmits to server equipment 3 at step S23, he is trying to maintain safety, as it re-enciphers using the public key of the equipment of a transmission place and digital data is transmitted since safety is low compared with the case of step S22.

[0072] Moreover, in step S27, since the equipment of a transmission place is not regular equipment when authentication of the equipment of a transmission place is not able to be taken, the 2nd authentication circuit 63 turns OFF connection between the regeneration circuit 16 and communication link I/F21. That is, the record regenerative apparatus 50 forbids the output of the enciphered digital data to the equipment of a transmission place.

[0073] When digital data can be transmitted in a completely safe environment, digital data can be safely transmitted [the above record regenerative apparatus 60] and received by permitting the output of the enciphered digital data only within the case where it outputs to the record regenerative apparatus 60 directly. Since it is transmitted to the record regenerative apparatus 50 of a transmission place, without the digital data saved at this time after having been enciphered by the storage section 15 carrying out re-encryption, the record regenerative apparatus 50 of a transmission place can output digital data to a high speed. Moreover, even if it is the case where it is not a direct output to the record regenerative apparatus 60, when authentication of the device of a transmission place is able to be taken, digital data can be transmitted to other equipments by carrying out re-encryption, securing safety. That is, in this example, the class of equipment which can be outputted rather than the example of drawing 6 and drawing 7 can be increased.

[0074] Next, the example of the record regenerative apparatus 70 into which an output method is changeable according to the description of the equipment of an output destination change is explained with reference to drawing 10 and drawing 11 . As a transmitting system which this record regenerative apparatus 70 is the record regenerative apparatus 2 shown in drawing 2 , and equipment which has the almost same configuration except for a transmitting system, and transmits the enciphered digital data to other equipments The authentication circuit 71 which takes authentication of the equipment of a transmission place, and the distinction circuit 72 which distinguishes the class of equipment of a transmission place according to the authentication result in the authentication circuit 71, It has the decryption circuit 73 which decodes the code of the enciphered digital data which was outputted from the regeneration circuit 16, and the re-encryption circuit 74 which re-enciphers the digital

data decrypted in the decryption circuit 73. Moreover, the record regenerative apparatus 70 is equipped with the decryption circuit 75 which decodes the code of the digital data outputted from the regeneration circuit 16 as analog output, and D/A converter 76 which changes the decrypted digital data into analog data.

[0075] The authentication circuit 71 attests the equipment of a transmission place. The authentication circuit 71 attests whether it has authority with the just equipment of a transmission place, such as whether to be the record regenerative apparatus 70 whose equipment of a transmission place is the exclusive device of this system concretely, or to be the record regenerative apparatus 60 or the general-purpose device to which the software for using this system was connected through whether they are general-purpose devices, such as a personal computer installed in normal, and server equipment 3. And the authentication circuit 71 outputs the class and authentication result of equipment which were able to take authentication to the distinction circuit 72.

[0076] The distinction circuit 72 distinguishes the class of equipment of the transmission place which transmits the enciphered digital data according to the output from the authentication circuit 71. And the distinction circuit 72 connects the regeneration circuit 16 and communication link I/F20, when transmitting digital data to the record regenerative apparatus 70 which was able to take authentication directly. Moreover, when transmitting digital data to a general-purpose device directly, the distinction circuit 72 connects the regeneration circuit 16 and the decryption circuit 73, indirect, i.e., when transmitting to the record regenerative apparatus 70 or a general-purpose device through server equipment 3. Furthermore, when the equipment which digital data transmits is not able to have namely, attest just authority, in order that the distinction circuit 72 may forbid the output of digital data or may carry out analog output, it connects the decryption circuit 75.

[0077] In case the decryption circuit 73 transmits digital data, it decodes the digital data enciphered in the encryption circuit 13 mentioned above in order to re-encipher, and outputs it to the re-encryption circuit 75.

[0078] The re-encryption circuit 74 acquires a public key from the record regenerative apparatus and general-purpose device which were able to take authentication in the authentication circuit 71, and re-enciphers digital data using this public key. And the re-encryption circuit 74 outputs the re-enciphered digital data to communication link I/F21.

[0079] Moreover, the decryption circuit 75 decodes the digital data enciphered in the encryption circuit 13 mentioned above in order to carry out analog output, and outputs it to D/A converter 76. And D/A converter 76 changes digital data into analog data, and

outputs analog data.

[0080] Next, the procedure at the time of the record regenerative apparatus 60 transmitting digital data to other equipments is explained using drawing 9 . If transmitting actuation transmit the enciphered digital data which is memorized by the user at the storage section 15 is carried out, the authentication circuit 71 of the record regenerative apparatus 70 of a transmitting agency attests whether the equipment of the transmission place of digital data is equipment which has authority, and will output an authentication result and the class of equipment which was able to take authentication to a distinction circuit 72 in step S31. The distinction circuit 72 judges whether according to an authentication result, the digital data enciphered from the regeneration circuit 16 is outputted to the prohibition of whether it outputs to communication link I/F20 or it outputs to the encryption circuit 73, and an output, or the decryption circuit 75.

[0081] The distinction circuit 72 outputs the digital data which was outputted from the regeneration circuit 16 and which is enciphered to communication link I/F21 in step S32, when it judges that digital data is directly transmitted to the record regenerative apparatus 70 of a transmission place. In this case, the enciphered digital data which was read from the storage section 15 is transmitted to the record regenerative apparatus 60 of a transmission place from communication link I/F21 in the condition [being enciphered] from communication environment being performed in the safe condition. And since the record regenerative apparatus 70 does not perform re-encryption in case it transmits digital data, it can transmit digital data to a high speed. When reproducing this digital data, using a common key, the record regenerative apparatus 60 of a transmission place decodes a code, and is reproduced.

[0082] When it judges that the distinction circuit 72 transmits digital data to the record regenerative apparatus 70 or a general-purpose device through the general-purpose device and the server equipment 3 which were directly connected to the equipment of the transmitting origin which is equipment of a transmission place, in step S33, the regeneration circuit 16 and the decryption circuit 73 are connected. And the decryption circuit 73 decodes the digital data enciphered in the encryption circuit 13 mentioned above in order to re-encipher, and outputs it to the re-encryption circuit 74. In step S34, the re-encryption circuit 74 acquires the public key of the equipment of a transmission place. In step S35, the re-encryption circuit 74 is again enciphered using the public key which acquired the digital data decrypted in the decryption circuit 73. And communication link I/F20 transmits this re-enciphered digital data to the equipment of a transmission place. That is, when the equipment of a transmission place is a

general-purpose device or it transmits to server equipment 3, he is trying to maintain safety, as it re-enciphers using the public key of the equipment of a transmission place and digital data is transmitted since safety is low compared with the case of step S32.

[0083] In step S36, the distinction circuit 72 forbids the output of digital data in step S36, when it judges that the equipment of the transmission place of digital data is equipment which does not have authority. Or the distinction circuit 72 is permitted only within analog output in step S36. When performing analog output, the distinction circuit 72 connects the regeneration circuit 16 and the decryption circuit 75. And the decryption circuit 75 decodes the digital data enciphered in the encryption circuit 13 mentioned above in order to re-encipher, and outputs it to D/A converter 76.

[0084] In the above record regenerative apparatus 70, whenever [insurance] can be changed and outputted according to the class of equipment of a transmission place. That is, when transmitting digital data to the record regenerative apparatus 70 directly, since it is the data transmission between exclusive devices, whenever [insurance] is high. Therefore, he is trying for the record regenerative apparatus 70 to transmit the digital data enciphered by the storage section 51 to the record regenerative apparatus 70 of a transmission place as it is, without carrying out re-encryption, in order to shorten air time. Moreover, the case where software is installed unjustly etc. is assumed and, as for general-purpose devices, such as a personal computer with which software, such as decryption used by this system, was installed, whenever [insurance] is low compared with the data transmission between exclusive devices. Moreover, also when transmitting digital data to the record regenerative apparatus 70 or a general-purpose device through server equipment 3, there is a possibility that the equipment which accessed server equipment 3 unjustly may download, and whenever [insurance] becomes lower than transmission between exclusive devices. Then, the record regenerative apparatus 70 performs re-encryption using the public key of a transmission place, and he is trying to maintain whenever [insurance] in such a case.

[0085] In addition, although the case where enciphered digital data and data were transmitted above was explained, RSA cryptograph, an ellipse code, etc. may be used as a public key cryptosystem, and you may make it use EKB and MJR as the concrete approach of a code as a private key method with an encryption rate quicker than a public key system. For example, between exclusive devices, it is good to use the high public key system of whenever [insurance] using a public key system with quick code acceleration by the data transmission to a general-purpose device, or the data transmission through server equipment 3.

[0086] Next, when the unapproved copy prevention information that the copy of digital

data is restricted to the digital data transmitted to the record regenerative apparatus 2 as copyright management data is included, based on this unapproved duplicate prevention information, the record regenerative apparatus 2 which restricts record of digital data is explained with reference to a drawing.

[0087] This record regenerative apparatus 80 has the input terminal 81 into which the digital data enciphered and compressed from server equipment 3 is inputted, as shown in drawing 12 . Moreover, the decryption circuit 82 where this record regenerative apparatus 80 decodes the enciphered digital data as a recording system, The expanding circuit 83 which elongates the digital data compressed, and the extract update circuit 84 which extracts and rewrites unapproved copy prevention information out of digital data, It has the compression circuit 85 which compresses digital data, the encryption circuit 86 which enciphers the digital data compressed, the record processing circuit 87 which performs record processing to the enciphered digital data, and the storage section 88 which saves the enciphered digital data.

[0088] Moreover, the record regenerative apparatus 80 has the decryption circuit 90 which decodes the digital data which is enciphered as the regeneration circuit 89 as a reversion system, and is memorized by the storage section 88, the expanding circuit 91 which elongates the digital data compressed, D/A converter 92 which changes a digital signal into an analog signal, the analog output terminal 93 which outputs an analog signal, and the digitized output terminal 94 which outputs the digital data of the preceding paragraph of D/A converter 92. Moreover, the record regenerative apparatus 80 has the system controller 95 which controls the whole actuation.

[0089] Digital data, such as audio data which were enciphered and compressed from server equipment 3 or other record regenerative apparatus 2 and which were carried out, a video data, and image data, are inputted into an input terminal 81. Moreover, SCMS (Serial Copy Management System) information is recorded on this digital data by the water mark. The decryption circuit 82 decodes the enciphered digital data which was inputted from the input terminal 81, enables it to extract the unapproved copy prevention information included in digital data, and outputs it to the expanding circuit 83. The expanding circuit 83 ATRAC3 (Adaptive Transform Acoustic Coding 3: trademark), MPEG-2AAC (Motion Picture Expert Group 2 AdvancedAudio Coding: trademark), MP3 (MPEG-1 Audio Layer3: trademark), TwinVQ (Transform-Domain Weighted Interleave Vector Quantization: trademark), MSAudio (WMA:Windows Media Audio: trademark), Ogg The digital data compressed by methods, such as Vorbis (trademark), is elongated, and it outputs to the extract update circuit 84.

[0090] The extract update circuit 84 detects the water mark included in the digital data

with which decryption was carried out and data were elongated, and extracts SCMS information. This SCMS information is a preparing-in 2 bits of head of data copy prohibition flag, and becomes 2 bits of heads of data from "00" (digital copy authorization), "10" (ban on a digital copy) or, and "11" (a digital copy is accepted only at once).

[0091] And the extract update circuit 84 permits recording digital data on the storage section 88, when SCMS information is "00" and "11." Moreover, when SCMS information is "11", "11" is rewritten to "10." Moreover, the extract update circuit 84 forbids record of the digital data to the storage section 88, when SCMS information is "10." And the extract update circuit 84 outputs the digital data with which SCMS information was updated to the compression circuit 85.

[0092] In addition, SCMS information may be CGMS (Copy Generation Management System). In this case, into digital data, CCI (Copy Control Information) which consists of 2 bits of "11" (no digital copy is accepted), "10" (the digital copy beyond this is not accepted), "01" (a digital copy is accepted only once), and "00" (a digital copy is accepted freely) is embedded. Of course, as unapproved copy prevention information, it is limited to neither SCMS nor CGMS.

[0093] The compression circuit 85 is ATRAC3 which mentioned the digital data above, MPEG-2AAC, MP3, and TwinVQ and MS. Audio, Ogg It compresses by methods, such as Vorbis, and outputs to the record processing circuit 87. The record processing circuit 87 performs and makes binary error correction coding processing and modulation processing to the data inputted, for example. And the data with which record processing was performed are recorded on the record medium which constitutes the storage section 88 which consists of a hard disk, a recordable optical disk, a magneto-optic disk, etc. with record means, such as the magnetic head and an optical pickup. In addition, the storage section 88 may be built in the body of equipment, and may be removable to the body of equipment.

[0094] Moreover, by playback means, such as the magnetic head and an optical pickup, the data memorized by the storage section 88 are read from a record medium, and are outputted to the regeneration circuit 89. The regeneration circuit 89 makes an output binary from a playback means, performs recovery processing and error correction processing, and outputs them to the decryption circuit 90. The decryption circuit 90 decodes the digital data enciphered in the encryption circuit 86, and outputs it to the expanding circuit 91 so that the digital data enciphered can be reproduced.

[0095] The expanding circuit 91 is ATRAC3, MPEG-2AAC, MP3, and TwinVQ and MS. Audio, Ogg The digital data compressed by methods, such as Vorbis, in the compression

circuit 85 is elongated, and it outputs to D/A converter 92 or the digitized output terminal 94. D/A converter 92 changes the decrypted digital data into an analog signal, and outputs it to an analog output terminal 93. The data from which the loudspeaker is connected and the analog output terminal 93 was changed into the analog signal are transduced electroacoustically, and it is outputted from a loudspeaker.

[0096] A system controller 95 controls the whole equipment. For example, a system controller 95 controls the record processing circuit 87 to permit recording digital data on the storage section 88, when the SCMS information on the inputted digital data is "00" and "11", and when SCMS information is "10", it controls the record processing circuit 87 to forbid record of the digital data to the storage section 88. Moreover, a system controller 95 controls the extract update circuit 84 to rewrite "11" to "10", when SCMS information is "11."

[0097] In the system using the above record regenerative apparatus 80, digital data, such as audio data enciphered and enciphered by the predetermined method from record regenerative-apparatus 80a of a transmitting agency, upload to server equipment 3 first. The SCMS information mentioned above is included in this enciphered digital data. When the digital data to upload is data which accept a digital copy freely here, SCMS information is set to "00", when it is data which accept a digital copy only at once, SCMS information is set to "11", and SCMS information is set to "10" when it is what forbids a digital copy. Server equipment 3 will be temporarily memorized as it is in the storage section which consists of hard disks etc., if the digital data enciphered from record regenerative-apparatus 80a of a transmitting agency is received. That is, server equipment 3 does not have the function which decodes the enciphered digital data and is reproduced. Therefore, since server equipment 3 does not have possibility of decoding the digital data memorized in the storage section also in the future, and reproducing, it does not update SCMS information.

[0098] And as shown in drawing 13 , record regenerative-apparatus 80b of a transmission place downloads the digital data accumulated in server equipment 3 by accessing server equipment 3. Then, the downloaded digital data is inputted into the decryption circuit 82. Here, a system controller 95 is step S41, and judges whether the downloaded digital data is decipherable in the decryption circuit 82. And a system controller 95 progresses to step S46, when it progresses to step S42 when it can decode, and it cannot decode.

[0099] If the downloaded digital data is decoded, the decryption circuit 82 is outputted to the expanding circuit 83, and the expanding circuit 83 will elongate the compressed digital data, and it will output it to the extract update circuit 84. The extract update

circuit 84 extracts the water mark on which SCMS information was recorded, and inputs SCMS information into a system controller 95. A system controller 95 judges any of "00", "11", and "10" SCMS information is in step S42.

[0100] Based on the read-out result of the SCMS information in step S42, in step S43, a system controller 95 controls the record processing circuit 87 to permit recording digital data on the storage section 88, when SCMS information is "00."

[0101] Moreover, in step S44, a system controller 95 controls the extract update circuit 84 to rewrite "11" to "10" while controlling the record processing circuit 87 to permit recording digital data on the storage section 88, when SCMS information is "01." And the extract update circuit 84 rewrites SCMS information from "11" to "10" based on the command from a system controller 95.

[0102] And if record in the storage section 88 is permitted in step S43 and step S44, it will be outputted to the compression circuit 85, the extract update circuit 84 compresses digital data again, and outputs it to the encryption circuit 86, it will encipher by the predetermined method again and the compression circuit 85 will output the encryption circuit 86 to the record processing circuit 87. The record processing circuit 87 performs processing required for record, and outputs it to a record means. And a record means records the digital data by which code compression was carried out on the record medium which constitutes the storage section 88.

[0103] Moreover, in step S45, a system controller 95 controls the record processing circuit 87 to forbid recording digital data on the storage section 88, when SCMS information is "10." A system controller 95 makes an alarm display a display, when digital data cannot be recorded.

[0104] Moreover, in step S41, when it judges that a code is undecipherable in the decryption circuit 82, in step S46, the direct output of the system controller 95 is carried out to the record processing circuit 87. The record processing circuit 87 performs processing required for record, and outputs it to a record means, and a record means records the digital data by which code compression was carried out on the record medium which constitutes the storage section 88.

[0105] Next, when reproducing the digital data which was memorized by the storage section 88 by processing of the above-mentioned step S43 or step S44 and which was enciphered and compressed, after the digital data memorized by the storage section 88 is read by the playback means, regeneration is given in the regeneration circuit 16 and it is outputted to the decryption circuit 90 of a reversion system. And the decryption circuit 90 decodes the digital data enciphered in the encryption circuit 86, outputs it to the expanding circuit 91, and the expanding circuit 91 elongates the compressed digital

data, and it outputs it to D/A converter 92 or the digitized output terminal 94. And D/A converter 92 changes a digital signal into an analog signal, and outputs it to a loudspeaker through an analog output terminal 93.

[0106] When SCMS information is not updated but it downloads to the refreshable record regenerative apparatus 80, he is trying to update SCMS information by the above systems with the server equipment 3 which cannot decode the enciphered digital data. Therefore, in this system, also when digital data is transmitted and received through a network 5, a certain unapproved copy prevention information can be managed from the former.

[0107] In addition, this invention may combine the processing performed with the record regenerative apparatus 2 mentioned above, and the processing performed with the record regenerative apparatus 80. Namely, when transmitting the digital data which included unapproved duplicate prevention information through server equipment 3 to a transmission place, the record regenerative apparatus of a transmitting agency acquires the equipment individual key of a transmission place, enciphers digital data using this, and should just transmit it to the record regenerative apparatus of a transmission place through server equipment. And since server equipment does not have the regenerative function, it does not update unapproved copy prevention information, but the record regenerative apparatus of a transmission place should just update unapproved duplicate prevention information, when the code of the received digital data is decipherable.

[0108]

[Effect of the Invention] When transmitting the enciphered data which were recorded on the record medium to server equipment according to this invention, When authentication of the equipment of a transmission place is taken and authentication is able to be taken, the code of the enciphered data which were recorded on the record medium is decoded. Since data are re-enciphered using the proper key data acquired from the equipment of a transmission place and it transmits from an output means, even if data are temporarily recorded on server equipment and this data downloads to the terminal unit of a third person without authority Protection of copyright can be aimed at by preventing being reproduced.

[0109] Moreover, when unapproved duplicate prevention information is included in the data downloaded from server equipment according to this invention, a certain unapproved copy prevention information can be managed from the former by extracting and updating unapproved duplicate prevention information with the renewal means of an extract, whenever it is recorded on refreshable equipment.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing explaining the data transceiver system by which this invention was applied.

[Drawing 2] It is the block diagram of the record regenerative apparatus used for the above-mentioned system.

[Drawing 3] It is the block diagram of the encryption circuit which enciphers digital data.

[Drawing 4] It is the block diagram of a decryption circuit.

[Drawing 5] It is a flow chart explaining authentication processing of a record regenerative apparatus.

[Drawing 6] It is the block diagram of the record regenerative apparatus which is a dedicated device.

[Drawing 7] It is a flow chart explaining the procedure at the time of transmitting digital data to other equipments.

[Drawing 8] It is the block diagram of the record regenerative apparatus which is a dedicated device.

[Drawing 9] It is a flow chart explaining the procedure at the time of transmitting digital data to other equipments.

[Drawing 10] It is the block diagram of the record regenerative apparatus which is a dedicated device.

[Drawing 11] It is a flow chart explaining the procedure at the time of transmitting digital data to other equipments.

[Drawing 12] When digital data including the unapproved copy prevention information transmitted through the network is downloaded, it is the block diagram of the record regenerative apparatus which updates this unapproved duplicate prevention information.

[Drawing 13] It is a flow chart for explaining actuation of the record regenerative apparatus shown in drawing 12 .

[Description of Notations]

1 Data Transceiver System, 2 (2a, 2b) Record Regenerative Apparatus, 3 Server equipment, 5 A network, 11 An input terminal, 12 Input terminal, 13 An encryption circuit, 14 A record processing circuit, 15 The storage section, 16 Regeneration circuit, 17 A selector, 18 authentication circuits, 19 A decryption circuit, 20 Re-encryption

circuit, 21 Communication link I/F, 22 A decryption circuit, 23 D/A converter, 24 A loudspeaker, 25 An output terminal, 31 A random-number-generation circuit, 32 Function circuit, 33 The memory for contents keys, the memory for 34 common keys, 35 Memory for equipment individual keys, 36 An equipment common key generation circuit, 37 contents encryption circuit, 28 Contents key encryption circuit, 41 A function circuit, 42 The memory for equipment individual keys, 43 Equipment common key generation circuit, 44 An encryption key decode circuit, 45 A contents decode circuit, 46 Memory for equipment common keys, 47 A selector, 80 A record regenerative apparatus (80a, 80b), 81 Input terminal, 82 A decryption circuit, 83 expanding circuits, 84 An extract detector, 85 Compression circuit, 86 An encryption circuit and 87 A record processing circuit, 88 The storage section, 89 A regeneration circuit, 90 A decryption circuit, 91 expanding circuits, 92 A D/A converter, 93 An analog output terminal, 94 A digitized output terminal, 95 System controller

---